

الخصوصية وامن المعلومات في الاعمال اللاسلكية بواسطة الهاتف الخلوي

المحامي يونس عرب

الاعمال الالكترونية اللاسلكية ، احد تجليات حالة الدمج بين نظم الحوسبة والاتصال ، بل هي فتح جديد من فتوح التقنية في حقلي الاتصال والحوسبة ، وتعد ابرز تطبيق لفكرة تكاملية وسائل تقنية المعلومات وتسهيل استخدام فتوحها في جهاز واحد . فتقنية المعلومات استلزمت ضمن مسيرة تطورها ، جهودا مبدعة في حقل صناعة الحواسيب ومكوناتها المادية (كاجهزة) وفي حقل صناعة البرمجيات (التي مثلت الدم الحي والمتدفق لنظم المعلومات واتاحت عبر تطبيقاتها اوسع افادة من اجهزة الكمبيوتر . واما نظم ووسائل الاتصالات ، فقد شهدت تطورا مذهلا نقلها من الاستخدام البدائي لشبكات التلغراف ، مرورا باستخدام انماط متعددة كالاسلاك النحاسية فالضوئية وغيرها - تنامت من حيث السعة والكفاءة - من اجل فعالية وسرعة وسائل التخابر ونقل البيانات ، الى ان وصلت الى مرحلة الاتصال عبر الاقمار الصناعية ونقل البيانات عبر شبكات الهاتف ومختلف ووسائل الائتمار عن بعد والتبادل الاتصالي اللاسلكي الذي يجد تجليه في وقتنا الحاضر بظاهرة (الهاتف الخليوي) .

ان الدمج والتزاوج بين وسائل الحوسبة والاتصال ، افرز مفهوما جديدا لكل منهما وخلق اطارا اوسع يعرف بتقنية المعلومات في وقتنا الحاضر ، ويسم العصر الذي نحيا ، هذا التزاوج الذي قام على فكرة توفير وسائط وبيئات لمعالجة البيانات وتبادلها ، وكانت شبكات المعلومات – وفي مقدمتها الانترنت – العنوان الجديد لعصر المعلومات اتاحت وتتيح التبادل الواسع لمختلف انماط المعلومات وتتيح التراسل الفوري ، وفي الوقت ذاته خلقت بيئة للاستثمار والاعمال فيما يعرف بالاسواق الافتراضية او بيئة الاعمال الالكترونية .

لقد انطلقت الاعمال الالكترونية بمختلف صورها ونمت بشكل واسع ، فتنامي سوق التجارة الالكترونية (البيع والشراء للسلع والخدمات على الخط) وتنامت الاعمال الالكترونية ما بين المؤسسات الانتاجية والخدمية ، وفي تجل جديد للوصول الى الزبون ولربطه بمؤسسات العمل والانتاج ، برزت ظاهرة الهواتف الخلوية التي تتيح تلقي المعلومات المالية والاستثمارية واستعراض مواقع مؤسسات الاعمال على سبكة الانترنت بفضل بروتوكولات اتصالية ملائمة مثل (الواب Wab) وبلوموث وغيرهما . ويعد اوسع تطبيق للاعمال الالكترونية بواسطة الهواتف الخلوية (كاهم وسيلة لاسلكية في الوقت الحاضر) الاعمال المصرفية الالكترونية او ما يعرف ببنوك الواب او بنوك الخليوي.

ولان تقنية المعلومات عموما ، افرزت ولا تزال تفرز تحديات قانونية ، فان الجهات التشريعة والقانونية في النظم المقارنة اولت اثار تقنية المعلومات على النظم القانونية عناية استثنائية وذلك لجهة تنظيم اثرها وايجاد البيئة الملاءمة لضمان سلامة استخدام التقنية وتشجيع اعتمادها وسيلة للاداء والانتاج . ومن بين اكثر التحديات القانونية اثارة للجدل وتاثيرا على الثقة بالتقنية وتطبيقاتها مسائل امن المعلومات والخصوصية .

ان هذه الورقة تهدف الى الوقوف على ابرز التحديات القانونية للخصوصية وامن المعلومات في بيئة الاعمال الالكترونية اللاسلكية ، اما المعالجة التفصيلية فانها امر متعذر في ضوء مساحة البحث المتاحة ، بحيث نكتفي بالاطر الرئيسة محيلين القاريء الكريم الى الابحاث والدراست التفصيلية في هذا الحقل . [1]

[1] انظر مؤلفنا قانون الكمبيوتر – مشار اليه فيما تقدم ، اضافة الى الاجزاء الاربعة التفصيلية من موسوعتنا القانون وتقنية المعلومات – اتحاد المصارف العربية .

1- القانون وتقنية المعلومات (اطار التاثر واحتياجات التدخل)

ان القراءة التاريخية التحليلية لحركة التشريع في حقل قانوني معين تقدم اساسا هاما لتحقيق رؤية شاملة في التعامل مع هذا الحقل ، مسائله وتحدياته وبدونها ، ربما لا يتحقق الانسجام والتناغم في الحلول والتدابير التشريعية التي تستهدف تنظيم هذا الحقل ، ومن أسف ان التعامل مع تشريعات تقنية المعلومات في غالبية النظم ، وربما حتى في اكثر الدول تقدما وانشطها في حقل تنظيم مسائل تقنية المعلومات ، بقي ضمن رؤى جزئية جاءت قاصرة عن الاحاطة الشاملة بالمتطلبات التشريعية والقانونية لهذا الحقل ، اذ يلحظ الدارس ان التعامل مع تقنية المعلومات تشريعيا تم خلال حقب زمنية متباينة وتناول قطاعات او موضوعات دون غيرها .

ففي ميدان امن المعلومات وجرائم الكمبيوتر مثلا ، تم التعامل مع الحماية الجنائية للمعلومات ضمن ثلاث محاور منفصلة ، اولها :- حماية البيانات الشخصية المخزنة في نظم المعلومات من مخاطر المعالجة الالية ، وهو ما يقع ضمن دراسات حقوق الانسان باعتباره ينصب على حماية الحق في الخصوصية Privacy أو الحياة الخاصة ، وثانيها :- حماية المعلومات ذات القيمة المالية او التي تمثل اصولا مالية من مخاطر الانماط الجرمية المستجدة التي تعتمد الكمبيوتر وسيلة للجريمة او هدفا او بيئة لها ، وهو ما عرف ايضا بجرائم الكمبيوتر Computer Crimes أو الجرائم المرتبطة بالكمبيوتر Computer-Related Crimes او جرائم الكمبيوتر ذات الطبيعة الاقتصادية Economic Computer Crimes , او غير ذلك من اصطلاحات دالة عليها، ويقع ضمن نطاق دراسات القانون الجنائي الموضوعي وهو ما عبر عنه بالعموم بوصفه الحق في المعلومات وثالثها :- حماية برامج الحاسوب من مخاطر القرصنة المتمثلة بالنسخ غير المصرح به واعادة الانتاج والتقليد وهو ما يقع ضمن دراسات الملكية الفكرية وتحديدا حقل حماية حق المؤلف Copyright .

ان محاولة تقصي التدابير التشريعية في حقل تقنية المعلومات يعني العودة الى بداية السبعينات ، فلماذا السبعينات ان التطور التاريخي لتقنية المعلومات ، يشير الى ان السبعينات تحديدا شهدت انتقالا حقيقيا في ميدان استخدام الحوسبة وتقاربها بانظمة الاتصالات ، فالسبعينات شهدت التوجه نحو بناء الحواسيب الشخصية وشهدت اتساعا تجاريا حقيقيا في استخدام الحوسبة ، وشهدت انجازات في حقل تشبيك الحواسيب وربطها مهدت لولادة عصر الشبكات. وبالرغم من ان العديد من المسائل المتصلة باستخدام الكمبيوتر قد اثيرت منذ الخمسينات والستينات ، - الا ان تلك المعالجات لم تؤد الى اتخاذ تدابير تشريعية ، لتكون ولادة القوانين الحقيقية ذات الصلة بالكمبيوتر قد تحققت مع مطلع السبعينات .

وتأقيت ولادة قانون الكمبيوتر او لنقل ملامحه الاولى بدأ مع شيوع استعمال الكمبيوتر وانخفاض كلفه ، ولأنه اداة جمع ومعالجة للمعلومات فقد كانت اول تحدياته القانونية اساءة الاستخدام على نحو يضر بمصالح الافراد والمؤسسات ، ومعه نشأ الارتباط بين القانون والكمبيوتر الذي انطلق من التساؤل فيما اذا كانت انشطة اساءة استخدام الكمبيوتر تقيم مسؤولية قانونية ام انها مجرد فعل غير مرغوب به اخلاقيا ؟ وما اذا كان يتعين تنظيم استخدام الكمبيوتر ام لا ؟؟ وهذا التساؤل اثير في حقلين ، الاول :- المسؤولية عن المساس بالافراد والمؤسسات عند اساءة التعامل مع بياناتهم الشخصية المخزنة في نظم الكمبيوتر على نحو يمس اسرارهم وحقهم في الخصوصية ، والثاني :- المسؤولية عن الافعال التي تمس او تعتدي على اموال الافراد ومصالحهم وعلى حقهم في المعلومات ذات القيمة الاقتصادية ، ولو دققنا في هذين الحقلين لوجدنا انفسنا امام (الخصوصية) و (جرائم الكمبيوتر -) .

اذن ثمة حقيقة اولى ان ولادة قانون تقنية المعلومات ارتبط بالبحث في المسؤولية عن انشطة تتصل بالمعلومات ونظمها وتحديدا في الحقل الجزائي .

والجدل الذي دار في ذلك الوقت (الستينات تحديدا وامتد الى مطلع السبعينات) اشبه بالجدل الدائر منذ نحو خمس سنوات بشأن الانترنت واسواق تقنية المعلومات :- هل يتعين اخضاع التقنية الجديدة ، توظيفها واستخدامها - للتنظيم القانوني ام تترك للتنظيم الذاتي ، او كما يعبر عنه الفكر الراسمالي (تنظيم السوق نفسه) فلا نكون امام قواعد قانونية تقر من الاطر الحاكمة بل امام قواعد سلوكية وشروط عقدية .

في هذا الاطار فان اول حالة موثقة لاساءة استخدام الكمبيوتر ترجع الى عام 1958 وفقا لما نشره معهد ستانفورد في الولايات المتحدة الامريكية ، ليبقى الحديث من ذلك الوقت وحتى مطلع السبعينات في اطار البعد الاخلاقي وقواعد السلوك المتعين ان تحكم استخدام الكمبيوتر ، ولتتجه الجهود والمواقف نحو حسم الجدل باعتبار اساءة استخدام الكمبيوتر فعلا موجبا للمسؤولية القانونية ، ولتنطلق التشريعات الوطنية في حقل جرائم الكمبيوتر مع نهاية السبعينات (تحديدا في الولايات المتحدة ابتداء من 1978) . اما الجهد الدولي فقد تحقق ابتداء في حقل الخصوصية ، ففي عام 1968 ، شهد مؤتمر الامم المتحدة لحقوق الانسان ، طرح موضوع مخاطر التكنولوجيا على الحق في الخصوصية ، اذ بالرغم من ان الحق في الخصوصية نشا قبل هذا التاريخ وحظي بجدل قانوني وقضائي وفكري منذ مئات السنين ، فانه لم يكن ثمة اثارة لما يتصل بهذا الحق متعلقا بالمعلومات الشخصية المعالجة آليا بالقدر الذي اثير في المؤتمر المشار اليه ، والذي استتبعه اصدار الامم المتحدة - كما سنرى - قرارات في هذا الحقل لتشهد بداية السبعينات (تحديدا عام 1973 في السويد) انطلاق تشريعات قوانين حماية الخصوصية مع الاشارة الى انها نوقشت في نظم قانونية اجنبية كثيرة - كدول اوروبا الغربية مثلا - ضمن مفهوم حماية البيانات Data Protection.

اذن الحقيقة الثانية ، ان الخصوصية وحماية البيانات تمثل اول حقل من حقول قانون تقنية المعلومات من حيث الاهتمام التنظيمي الدولي مع انها ترافقت مع الحديث حول جرائم الكمبيوتر وكما يظهر من تواريخ انطلاق التشريعات الوطنية فانهما سارا معا من حيث التدابير التشريعية الوطنية مع اسبقية لتشريعات الخصوصية طبعا مع موجة تشريعات الحماية القانونية للبرمجيات كما سنرى .

ولأن السبعينات شهدت بحق الادراك العميق لأهمية برامج الكمبيوتر وباتت تشير الى انها ستكون القيمة الاكثر اهمية من بين عناصر تقنية المعلومات وستفوق عتاد الكمبيوتر المادي في اهميتها ، بدات تظهر التدابير التشريعية في حقل حماية البرمجيات اعتبارا من 1973 (في الفلبين) مع ان موجة هذه التشريعات يتم ارجاعها للثمانينات لان الاخيرة شهدت تدابير تشريعية وطنية واسعة في حقل حماية البرمجيات بسبب الاثر الذي تركته القواعد النموذجية لحماية برامج الكمبيوتر الموضوعة من خبراء المنظمة العالمية للملكية الفكرية (الوايبو) عام 1978

وصحيح ان تشريعات حماية البرامج ترافقت مع تشريعات الخصوصية وجرائم الكمبيوتر ، لكنها كانت اسرع تناميا واوضح من حيث الرؤى للمحتوى ولمستقبل هذه التشريعات ، ولهذا فانها اوسع مدى من حيث عددها واذا اردنا ان نعرف السر فانه في الحقيقة يرجع الى عاملين أساسيين ، الاول:- وجود المنظمة العالمية للملكية الفكرية (الوايبو) ، التي ساهمت عبر ملتقياتها وادلتها الارشادية وقوانينها النموذجية في حسم الجدل بشان موضع حماية البرمجيات ليكون قوانين حق المؤلف . والثاني :- التوجه الاستراتيجي للاسواق الراسمالية للاستثمار في حقل الملكية الفكرية ومصنفاتها كمقدمة لبناء الاقتصاد الرقمي الذي بدأت اول ملامحه في اتجاه الولايات المتحدة الامريكية مدفوعة بتأثير الشركات متعددة الجنسيات لوضع الملكية الفكرية ضمن اجندة اتفاقيات تحرير التجارة والخدمات ومساومة الولايات المتحدة العالم كله على قبول اتفاقيات تحرير التجارة في البضائع مقابل انجاز تقدم في حقلي تحرير الخدمات والملكية الفكرية .

ولا يعني هذا ان بقية موضوعات تقنية المعلومات لم تحظ بدعم واهتمام هيئات دولية ، لكن الفرق ان ايا منها حتى ذلك الوقت لم يكن موضع عمل منظمة متخصصة فيه كما هو حال منظمة الوايبو التي تتولى رعاية الملكية الفكرية وادارة اتفاقياتها .

اذن الحقيقة الثالثة ، ان اكثر تشريعات قانون تقنية المعلومات نضجا ووضوحا في اغراضها القوانين او التدابير التشريعية المتعلقة بحماية الملكية الفكرية لبرامج الكمبيوتر (وفيما بعد قواعد البيانات والدوائر المتكاملة) ويتصور ان تحقق هذه التشريعات ايضا حماية اوسع في السنوات القادمة في حقل اسماء مواقع الانترنت والمحتوى الرقمي لمواقع الانترنت .

ثلاثة موجات تشريعية :- تشريعات الخصوصية (حماية الحق في البيانات الشخصية من مخاطر التكنولوجيا) ، قوانين جرائم الكمبيوتر (الاعتداء على نظم المعلومات والمعلومات ببعدها الاقتصادي) وتشريعات حماية برامج الكمبيوتر (الملكية الفكرية) .هذه حقول ثلاثة في ساحة قانون تقنية المعلومات ، وسنجد بعد قليل ان ثمة حقل رابع يكاد يكون الوعاء الذي يضمها جميعا وهو حقل الاعمال الالكترونية ، لكن يفصل بين حقل الاعمال الالكترونية والحقول الثلاثة ، حقول اخرى ربما لا تكون مستقلة بشكل كاف في مبناها عن الفروع القانونية التي تتبعها لكنها بالتاكيد خلقت تغيرات جوهرية استلزمتها تقنية المعلومات .

فأول الحقول التي برزت عقب الحقول الثلاثة المتقدمة ، قواعد الاجراءات الجنائية للاستدلال والتحقيق والاثبات وإجراءات المحاكمة المتفقة مع طبيعة الاعتداءات في الدعاوى التي تتعلق بجرائم الكمبيوتر او الاعتداء على الخصوصية وحتى في حقل قرصنة برمجيات الحاسوب المخزنة داخل النظم او المحملة مع الاجهزة . وبالرغم من ان الدول الاوروبية واستراليا كذلك قد تنبهت لهذا الموضوع مبكرا مع مطلع السبعينات الا ان الموجة التشريعية المتصلة بهذه القواعد بدات حقيقة وعلى نطاق واسع في منتصف الثمانينات .وتبع هذا الحقل تدابير تشريعية في ثلاثة حقول اخرى كان للانترنت وشبكات المعلومات ونماء استثمارات الخدمات التقنية الدور في توجيه الاهتمام الحقيقي بها، بل في ولادة مفهوم جديد لبداياتها التي ظهرت قبل شيوع الانترنت ، فمع تحول الانترنت الى الاستخدام التجاري الواسع ، ظهرت تحديات قانونية جديدة ، بعضها ذو اتصال بتحديات سابقة أو قائمة ، كتحديات حماية امن المعلومات في حقلي الخصوصية وجرائم الكمبيوتر وحماية البرامج في بيئة الانترنت ذاتها ، لما اتاحته من تسهيل ارتكاب الاعتداءات بعد ان وفرت مدخلا سهلا الى نظم الكمبيوتر المرتبطة ضمنها . وتحديات اخرى أوجبتها انماط السلوك الجدية التي ولدت بولادة الانترنت ، كالبيع والشراء على الشبكات واداء الخدمة عبر الانترنت ، ومن هذه التحديات التنظيم القانوني للتجارة الالكترونية . هذه التحديات التي اوجدتها او ضخمتها الانترنت او عدلت في نطاقها ومخاطرها وجديتها ، رافقها موجات تشريعية بدات في حقل ما يعرف بتنظيم الامن المعلوماتي والمعايير التقنية وتحديدا ما يتصل بتشفير البيانات ، التي انطلقت في عام 1990 من فرنسا تحديدا ، ثم في حقل مكافحة المحتوى غير القانوني للمعلوماتية ، الذي انطلق عام 1996 في امريكا . واخيرا الحقل الاكثر اثارة للجدل واوسعها تنظيما ، حقل الاعمال الالكترونية الذي اشرنا اعلاه الى انه الحقل الرابع المركزي الى جانب جرائم الكمبيوتر والخصوصية والملكية الفكرية . وحقل الاعمال الالكتروني ليس لاحقا للحقول الاخيرة الثلاث ، انما قد نجد تشريعات في اطاره ، كالتشريعات المتعلقة بتقنيات الاعمال المصرفية ، او تلك المتعلقة بحجية الاثبات بالوسائل الالكترونية ، سابق بسنوات عديدة للحقول المشار

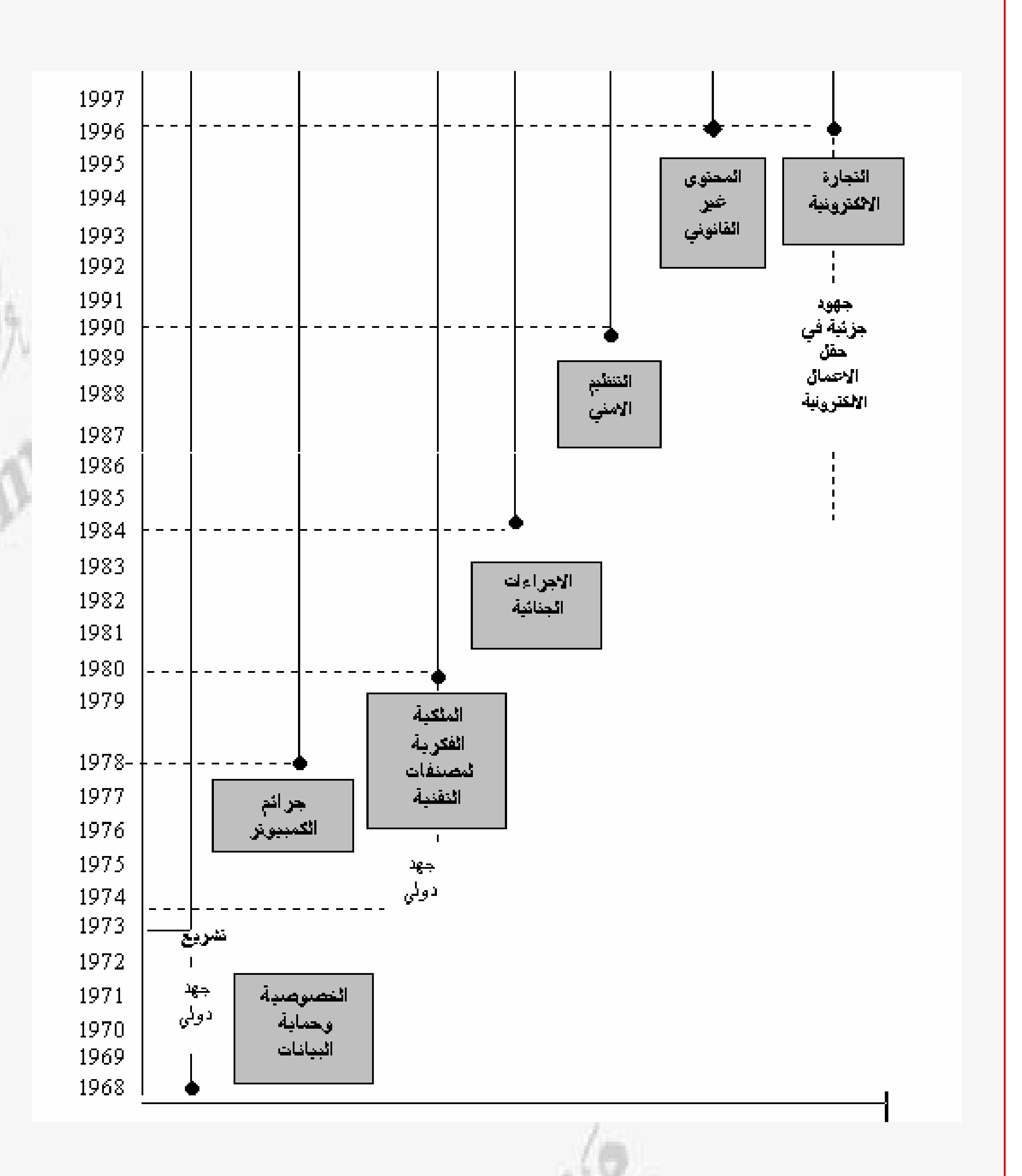
اليها ، لكن قولنا بانه الحقل الاخير زمنيا يرجع الى تبلور مفاهيم شمولية جديدة في حقل الاعمال الالكترونية عكسها تحديدا مفهوم التجارة الالكترونية والبنوك الالكترونية . وهذا المفهوم الشامل نجد انه انطلق مع عام 1996 الذي شهد اقرار القانون النموذجي للتجارة الالكترونية من قبل لجنة الامم المتحدة لقانون التجارة (اليونسترال) . ونجد ان دولا على المستوى التشريعي كانت قد بدات الاهتمام بمسائل الاعمال الالكترونية (كالاثبات بالوسائل الالكترونية وحجية مستخرجات الحاسوب والتنظيم القانوني لبطاقات الائتمان وغيرها) من اواخر السبعينات وبداية الثمانينات ، لكنها لم تكن ضمن التصور الشامل للتجارة الالكترونية التي ارتبطت واقعا بانشطة الاستثمار على الانترنت .

اما من حيث الاطر الدولية العاملة في ميادين الموضوعات المتقدمة ، فاننا نجد الجهد الاساسي والمميز موزع بين منظمة التعاون الاقتصادي والتنمية وهيئات اوروبا (مجلس اوروبا والمفوضية الاوروبية واتحاد اوروبا والبرلمان الاوروبي) والامم المتحدة ، ومجموعة الدول الصناعية الثمانية والوايبو ، والانتربول ، ومنظمة التجارة الدولية وغيرها من المنظمات.

اذن هذا خط اندلاع موجات تشريعات قانون الكمبيوتر :-

الخصوصية ، جرائم الكمبيوتر ، الملكية الفكرية للمصنفات الرقمية ، الاجراءات الجنائية في البيئة الرقمية ، المعايير والمواصفات والاطر التنظيمية للتقنية وتاثيرها على النشاط الاداري والخدمي ، المحتوى غير القانوني للمعلوماتية ، الاعمال الالكترونية وتحديدا التجارة الالكترونية ، وفي اطار كل منهما ثمة تشريعات ومجهودات دولية واقليمية وسياسات واستراتيجيات ومحتوى ومشكلات ايضا . (انظر شكل رقم 1)

الشكل رقم 1



2- عناصر حماية نظم المعلومات بوجه عام

مع تزايد القيمة الاقتصادية والمالية للمعلومات ، وشيوع وتنامي التطبيقات العملية لفكرة راس المال الفكري والاقتصاد القائم على المعرفة او الاقتصاد الرقمي ، وجب العمل على توفير الحماية التقنية لنظم المعلومات وهو ما ادى الى ابتكار وسائل تقنية متنامية كجدران النار وكلمات السر ووسائل التعريف البيولوجية والتشفير وغيرها ، الا ان الحماية التقنية ليست كافية لضمان حماية المعلومات ونظمها وتطبيقاتها ، عوضا عن انها لم تؤد الى توفير ثقة واسعة بنظم التقنية لدى المستخدمين الذين تسود عندهم قناعة ان نظم الكمبيوتر والانترنت ووسائل الاتصال اللاسلكي ليست أمنة بقدر الوسائل التقليدية للاعمال القائمة على الورق والدليل الكتابي او المادي ، لهذا كان لزما ان تتحرك النظم القانونية لضمان توفير حماية للمعلومات .

وبشكل عام ، ودون الخوض في تفاصيل عناصر الحماية ، فان مختلف وسائل الحماية (القتنية والقانونية) تهدف الى تامين الحماية في الموضع التالية والتي تمثل في القوت ذاته عناصر النظام الامني للمعلومات :-

1-2 Authentication وهي القدرة على اثبات شخصية الطرف الاخر على الشبكة وبنفس الوقت اثبات شخصية الموقع للمستخدم .

2-2 Privacy الخصوصية او حماية بيانات المستخدم من الافشاء والاطلاع دون اذن او تخويل.

3-2 Access Control الصلاحيات وتحديد مناطق الاستخدام المسموحة لكل مستخدم واوقاته .

Integrity (تكاملية او سلامة المحتوى) وتتصل بالتاكد من ان المعلومة التي ارسلت هي نفسها التي تم تلقيها من الطرف الاخر .

Non-repudiation (عدم الانكار) اذ لا يكفي فقط اثبات شخصية المستخدم او الموقع بل يتعين ضمان عدم انكار منفذالتصرف صدور التصرف عنه .

AVAILABILITY استمرارية توفر المعلومات او الخدمة ، اذ لا يكفي الوجود وتقديم الخدمة الالكترونية ووجود النظام الالكتروني ويتعن ضمان استمرار الوجود وحماية النظام من انشطة التعطيل (كهجمات انكار الخدمة)

3 - الاطار القانوني لحماية نظم المعلومات وتنظيم استخداماتها .

ان اخطر ما يواجه فعالية نظم حماية المعلومات وفعالية الادوات التشريعية لتنظيم استخداماتها و تطبيقاتها وصورها المعالجات الجزئية للتحديات القانونية المتصلة بتقنية المعلومات ، اذ تظهر الدراست التحليلة اهمية الحاجة الى حزمة متكاملة من التشريعات في حقل تقنية المعلومات ، تمتد لتغطية عناصر اساسية اربعة :-

الاعتراف القانوني بالمعلومات ووسائل حمايتها في النظام القانوني .

التنظيم الملائم لوسائل التقنية ومعاييرها ومواصفاتها .

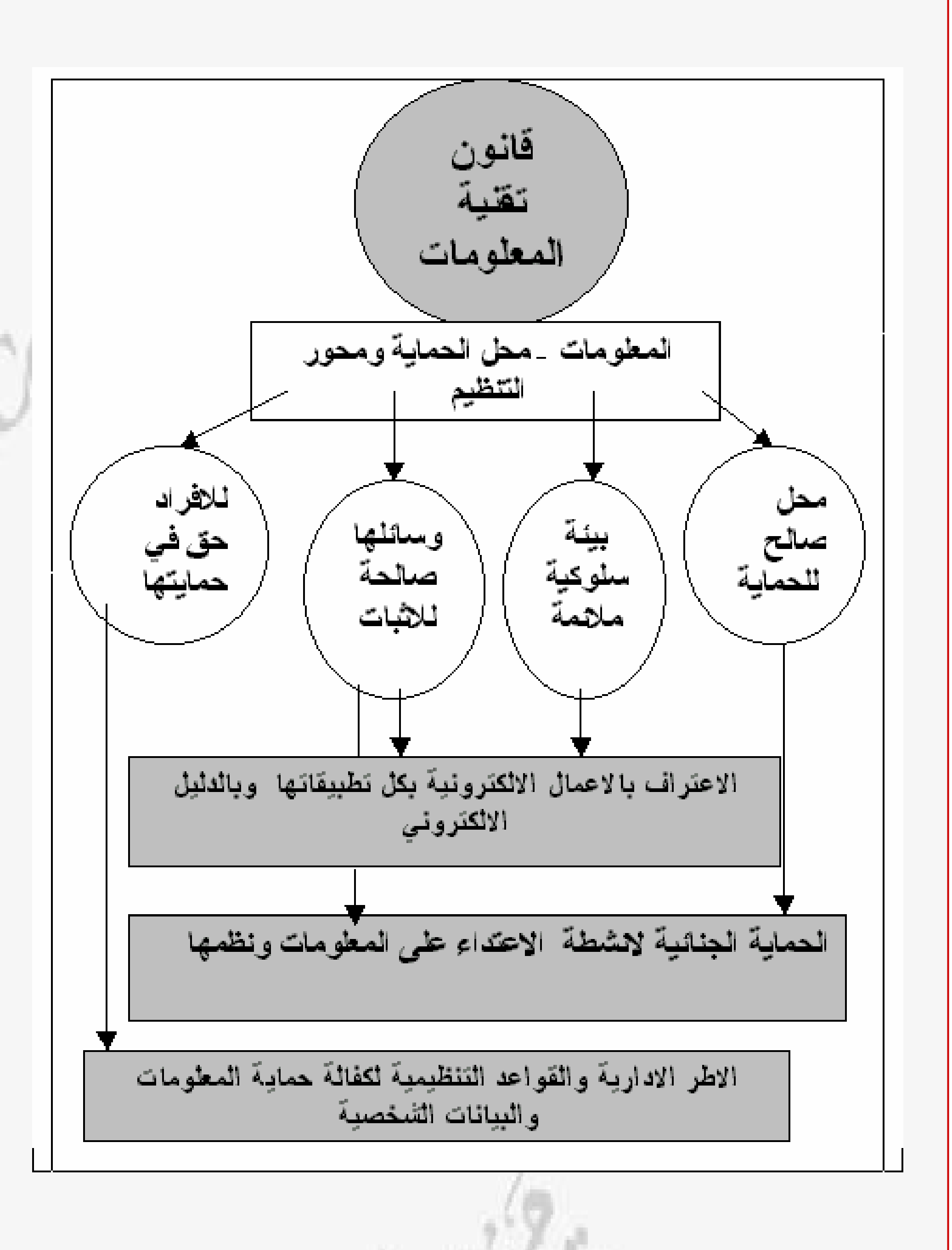
الاعتراف القانوني بصلاحية الوسائل الالكترونية في بيئة الاعمال والخدمات والاستثمار .

الاعتراف القانوني بمصالح المستهلك والمستخدم وتوفير الحمتية القانونية من عيوب ومخاطر التقنية وتطبيقاتها .

وهذه العناصر الاربعة تمثل الاطار القانوني الذي تندرج في نطاقه مختلف تشريعات تقنية المعلومات ، بحيث لا تكون حزمة التشريع فاعلة او كافية ما لم تضمن حماية المعلومات ذاتها من انشطة الاعتداء عليها ، وحماية المستخدم من مخاطر التقنية وتخلف المواصفات وما قد يتعرض له من انشطة جرمية . وتوفير بيئة ملائمة للاعمال الالكترونية بمختلف تطبيقاتها من خلال الاعتراف بالوسائل الالكترونية بمختلف انواعها للتعاقد والاثبات وتوفير معايير سلامة النشاط التجاري والاستثماري في البيئة الافتراضية بذات القدر الذي تحظى به في بيئة العالم الحقيقي او الورقي .

ولان المقام لا يحتمل الوقوف التفصيلي على محتوى هذا الاطار وتفرعاته ، فاننا نكتفي بالقدر المتقدم ونحيل القاريء الكريم الى ما سبق لنا الاشارة اليه من مراجع متخصصة في هذا الحقل مما وفقنا الله لوضعها . ويوضح الشكل 2 تاليا ، التصور العام للاطار القانوني لحماية المعلومات الذي يمثل في الوقت ذاته اطار قانون تقنية المعلومات .

شكل 2 :-



4- الخصوصية – ماهيتها ، مصادر التهديد في بيئة الاعمال الالكترونية اللاسلكية ، اتجاهات ومتطلبات الحماية .

4-1 المعنى والخلفية التاريخية :-

ان الحق في الخصوصية ، او كما يعرف في النظام اللاتيني بالحق في الحياة الخاصة ، يعرف بحق احترام سرية وخصوصية الاشخاص من اي تدخل مادي او معنوي ، وهو حق عميق الجذور من الوجهة التاريخية ، ففي الكتب السماوية ثمة العديد من الاشارات للخصوصية تنطوي على اعتراف بحماية الشخص من ان يكون مراقبا ، وثمة حماية للخصوصية في الشرائع اليونانية والصينية القديمة . وقد جاء القران الكريم[2] صريحا في حماية السرية وفي منع انشطة التجسس وكذلك في حماية المساكن من الدخول دون اذن .

---

[2] (يا ايها الذين آمنوا لا تدخلوا بيوتا غير بيوتكم حتى تستأنسوا وتسلموا على اهلها)) الاية 27 من سورة النور من القران الكريم ((ولا تجسسوا ولا يغتب بعضكم بعضا)) الاية 12من سورة الحجرات .

أما بالنسبة للتشريعات الوضعية فان الدول الغربية قد اقرت جوانب من حماية الخصوصية منذ مئات السنين ، ففي عام 1361 تم سن قانون في بريطانيا (The Justices of the Peace Act) يمنع اختلاس النظر واستراق السمع ويعاقب عليها بالحبس . وفي عام 1765 اصدر اللورد البريطاني Camden قراره بعدم جواز تفتيش منزل وضبط اوراق فيه[3]

وقد طورت عدد من الدول حماية متقدمة للخصوصية بعد هذا التاريخ ، ففي عام 1776 سن البرلمان السويدي قانون الوصول الى السجلات العامة والذي الزم كافة الجهات الحكومية التي لديها معلومات ان تستخدمها لاهداف مشروعة . وفي عام 1858 منعت فرنسا نشر الحقائق الخاصة وفرضت عقابا على المخالفين ، أما قانون العقوبات النرويجي فقد منع في عام 1889 نشر المعلومات التي تتعلق بالشخصية والاوضاع الخاصة.

وًفي عام 1890 كتب محاميان امريكيان Samual Warren and Louis Brandeis مقالا عن حماية الخصوصية باعتبار الاعتداء عليها من قبيل الفعل الضار ووصف الخصوصية بأنها الحق في ترك الشخص وحيدا ، وقد انتشر هذا المفهوم في الولايات المتحدة الامريكية كجزء من القانون العام .

وفي العصر الحديث فان مفهوم الحق في الخصوصية ظهر في الاعلان العالمي لحقوق الانسان 4 في عام 1948 والذي كفل حماية الاماكن والاتصالات.

كما ان العديد من اتفاقيات حقوق الانسان العالمية اعترفت بالحق في الخصوصية كالعهد الدولي للحقوق المدنية والسياسية (ICCPR) واتفاقية الأمم المتحدة للعمال المهجرين واتفاقية الأمم المتحدة لحماية الطفولة وغيرها .

وأما على المستوى الاقليمي فان العديد من الاتفاقيات اعترفت بالحق في الخصوصية ونظمت قواعد حمايته كما هي الحال في الاتفاقية الاوروبية لحماية حقوق الانسان والحريات الاساسية (روما لعام 1950) 5وهذه الاتفاقية قد انشأت المفوضية الاوروبية لحقوق الانسان والمحكمة الاوربية لحقوق الانسان لمراقبة تطبيقها وكلاهما كان نشطا في تطبيق وحماية الحق في الخصوصية وضيق من نطاق الاستثناءات على حكم المادة الثامنة وما تقرره من حماية ، وفي هذا الشأن فان المفوضية الاوروبية لحقوق الانسان قالت عام 1976 (ان الحق في احترام الحياة الخاصة هو الحق في الخصوصية ، الحق في الحياة الى المدى الذي يتمناه الانسان والحق في الحماية من العالمية) . ووفقا لرأي اللجنة فان الحق في احترام الحياة الخاصة لا ينتهي هنا بل يمتد الى الحق في تأسيس وتطوير العلاقات مع الاشخاص الاخرين .

أما المحكمة الاوروبية لحقوق الانسان ، فقد راجعت العديد من قوانين دول الاعضاء في معرض نظرها للدعاوى المقامة اليها وقررت ان العديد من الدول فشلت في تنظيم عمليات استراق السمع على نحو مس خصوصية الافراد وقد راجعت قضايا لأفراد من اجل حقهم للوصول الى المعلومات الخاصة بهم الموجودة في الملفات الحكومية لضمان صحتها وسلامة اجراءات المعالجة ، وقد طبقت حكم المادة الثامنة الى ابعد من الجهات الحكومية لتشمل الجهات الخاصة كلما ظهر ان على الحكومة ان تمنع اية اجراءات في القطاع الخاص تخالف المادة الثامنة.

اتفاقيات اقليمية اخرى ، بدأت تنص بوضوح على حماية الخصوصية ، كالمادة 11 من الاتفاقية الامريكية لحقوق الانسان التي جاء نصها مطابقا تقريبا للنص المقرر في الاعلان العالمي لحقوق الانسان .

وفي عام 1965 تبنت الولايات المتحدة الاعلان الامريكي للحقوق والواجبات الذي يتضمن مجموعة من الحقوق من بينها الحق في الخصوصية ، وقد بدأت المحاكم الامريكية الداخلية والمحكمة الامريكية لحقوق الانسان اظهار ومعالجة حق الخصوصية ومسائله فيما تنظر من دعاوى .

تطور الحق في الخصوصية وحماية البيانات في الستينات والسبعينات نتيجة للتأثر بتقنية المعلومات وبسبب القوى الرقابية المحتملة لانظمة الكمبيوتر التي استوجبت وضع قواعد معينة تحكم جمع ومعالجة البيانات الخاصة ، وفي هذا الحقل فان اول معالجة تشريعية في ميدان حماية البيانات كان عام 1970 في هيس بالمانيا (LAND OF HESSE IN GERMANY) والذي تبعه سن او قانون وطني (متكامل) في السويد عام 1973 ثم الولايات المتحدة عام 1974 ثم المانيا على المستوى الفدرالي عام 1977 ثم فرنسا عام 1978 وسنعود الى الاستعراض التفصيلي للتدابير التشريعية في حقل الخصوصية فيما ياتي .

---

[3] وتعليقا على هذا الحكم كتب WILLIAM PITT "قد يكون احد الفقراء في كوخه غير قادر على الدفاع عن ان يدخل الريح بيته او ان تحطمه العاصفة او ان يدخل المطر من سطح كوخه لكنه قادر على ان يحمي بسياجه المهدم نفسه في مواجهة قوة التاج ، ولا يستطيع ملك انجلترا الدخول ، فكل قوته العظيمة لن تستطيع ان تتجاوز عتبة المنزل المهدم . انظر :- The 2000 Privacy Report , the Electronic Privacy Information Center

[4] فقد نصت المادة 12 من الاعلان العالمي على انه ((لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات))

[5] حيث قررت في المادة الثامنة منها (1- لكل انسان الحق في احترام حرمة حياته الخاصة ، وحرمة منزله ومراسلاته . 2- يمنع تدخل السلطة العامة في ممارسة الانسان لحقه المذكور الا في الاحوال التي يبينها القانون ، وفي حالة حماية الامن القومي للمجتمع الديمقراطي ، او لحماية سلامة الناس او للمصلحة الاقتصادية او لمنع حالات الفوضى او ارتكب الجرائم ، او لحفظ الصحة والاخلاق العامة ، او لحماية ورعاية حقوق وحريات الاخرين) .

وفي عام 1981 وضع الاتحاد الأوروبي اتفاقية حماية الافراد من مخاطر المعالجة الالية للبيانات الشخصية ، ووضعت كذلك منظمة التعاون الاقتصادي والتنمية دليلا ارشاديا لحماية الخصوصية ونقل البيانات الخاصة ، والذي قرر مجموعة قواعد تحكم عمليات المعالجة الالكترونية للبيانات ، وهذه القواعد تصف البيانات والمعلومات الشخصية على انها معطيات تتوفر لها الحماية في كل مرحلة من مراحل الجمع COLLECTION والتخزين STORAGE والمعالجة PROESSING والنشر DISSEMINATION.

ومفهوم حماية البيانات في المواثيق المتقدمة والقوانين يتطلب ان تكون البيانات الشخصية :-

1 - قد تم الحصول عليها بطريق مشروع وقانوني .

2 - تستخدم للغرض الاصلي المعلن والمحدد

3 - تتصل بالغرض المقصود من الجمع ولا تتجاوزه ومحصورة بذلك .

4 - صحيحة وتخضع لعمليات التحديث والتصحيح .

5 - يتوفر حق الوصول اليها

6 - تحفظ سرية وتحمى سريتها .

7 - تدمر بعد استنفاذ الغرض من جمعها

وقد اثرت الاتفاقية الاوروبية ودليل منظمة التعاون الاقتصادي ايما تاثير وبشكل ادى الى وضع تشريعات في مختلف دول العالم ، وقد وقعت ما يقارب 30 دولة على الاتفاقية الاوروبية ، وكثير من الدول تخطط للانضمام اليها كما استخدم دليل منظمة التعاون الاقتصادي والتنمية بشكل واسع وتأثرت به العديد من التشريعات الوطنية حتى خارج اطار الدول الاعضاء في هذه المنظمة .

انواع ومفاهيم الخصوصية وتهديداتها

يمكن تقسيم الخصوصية الى عدد من المفاهيم المنفصلة لكنها ترتبط معا في الوقت ذاته وهي:-

1- خصوصية المعلومات Information Privacy والتي تتضمن القواعد التي تحكم جمع وادارة البيانات الخاصة كمعلومات بطاقات الهوية والمعلومات المالية والسجلات الطبية والسجلات الحكومية وهي المحل الذي يتصل عادة بمفهوم حماية البيانات Data Protiction .

2- الخصوصية الجسدية او المادية Bodily Privacy : والتي تتعلق بالحماية الجسدية للافراد ضد اية اجراءات ماسة بالنواحي المادية لاجسادهم كفحوص الجينات GENETIC TESTS ، وفحص المخدرات DRUG TESTING .

3- خصوصية الاتصالات Telecomunication Privacy والتي تغطي سرية وخصوصية المراسلات الهاتفية والبريد والبريد الالكتروني والاتصالات الخليوية وغيرها من الاتصالات .

4- الخصوصية الاقليمية (نسبة الى الاقليم المكاني) والتي تتعلق بالقواعد المنظمة للدخول الى المنازل وبيئة العمل او الاماكن العامة والتي تتضمن التفتيش والرقابة الالكترونية والتوثق من بطاقات الهوية .

وتمكن تقنية المعلومات الجديدة خزن واسترجاع وتحليل كميات هائلة من البيانات الشخصية التي يتم تجميعها من قبل المؤسسات والدوائر والوكالات الحكومية ومن قبل الشركات الخاصة ، ويعود الفضل لهذا الى مقدرة الحوسبة الرخيصة ، وأكثر من هذا فانه يمكن مقارنة المعلومات المخزونة في ملف مؤتمت بمعلومات في قاعدة بيانات أخرى ، ويمكن نقلها عبر البلد في ثوان وبتكاليف منخفضة نسبيا ، "أن هذا بوضوح يكشف الى أي مدى يمكن أن يكون تهديد الخصوصية "

وتتزايد مخاطر التقنيات الحديثة على حماية الخصوصية ، كتقنيات رقابة (كاميرات) الفيديو ، وبطاقات الهوية والتعريف الالكترونية ، وقواعد البيانات الشخصية، ووسائل اعتراض ورقابة البريد والاتصالات السلكية واللاسلكية ورقابة بيئة العمل وغيرها .

وقد اظهرت التقارير الصادرة عن هيئات ومنظمات حماية الخصوصية ان معلومات الافراد والمؤسسات ليست آمنة من الاطلاع عليها وافشائها ، وليست الخطورة فقط فيما يمكن الوصول اليه من معلومة في وقت معين ، اذ الخطورة الاكبر فيما يمكن جمعه من معلومات وتحليلها كحزمة واحدة للوصول الى حقائق عن الفرد تساهم في تنفيذ انشطة المساس به او الاعتداء على حقوقه الاخرى . وابرز مثال في هذا الحقل ، قدرة انماط من البرمجيات والنظم على تجميع عادات الشخص وحقائق معيشته على نحو قد يتيح في اي وقت الاعتداء على سمعته او كرامته او اعتباره المالي او يساهم في توفير فرصة حقيقة لاختراق نظامه او هاتفه الخلوي واستخدام بياناته السرية للوصول الى حساباته البنكية ومباشرة افعال اعتداء مختلفة عليها .

2-4 الانماط والنماذج التشريعية في حقل حماية البيانات :-

هناك ثلاثة نماذج تشريعية لتدابير حماية الخصوصية المعلوماتية ، وهذه التدابير تعتمد في تطبيقاتها على ما اذا كان منطلق النظام القانوني مجرد الاعتراف بالخصوصية معتمدا على اباحة كل ما يدخل في نطاق الحق ، او باستخدام وسيلة مواجهة الانشطة التي تمثل اعتداءا على الخصوصية ، وفي كثير من الدول يستخدم الاتجاهين معا وبالنسبة للدول التي توفر حماية فاعلة للخصوصية فانها قد تستخدم نموذجا او اكثر لضمان حماية الخصوصية وهذه النماذج هي : -

1 - القوانين الشاملة COMPREHENSIVE LAWS : في العديد من دول العالم ثمة قوانين عامة تحكم عمليات جمع وادارة ومعالجة البيانات الشخصية في القطاعين العام والخاص ، مع وجود جهة لضمان التواؤم مع القانون وتطبيقها ، وهذا هو النموذج الشائع في الدول التي تتبنى قوانين حماية البيانات كما هو حال دول الاتحاد الأوروبي ، وهي الدول المتعين عليها التوافق مع دليل حماية البيانات الارشادي الصادر عن الاتحاد الاوروبي. وقد تم وضع العديد من مثل هذه القوانين في دول خارج الاتحاد الأوروبي ايضا كما هو الحال في كندا واستراليا وتسمى ايضا هذه القوانين او توصف احيانا بأنها CO-REGULATORY MODEL

2 - القوانين القطاعية المخصصة SECTORAL LAWS : وهي التي تتعلق بقطاع معين ، اذ ان بعض الدول ، كما هو الحال في الولايات المتحدة الامريكية ، تجنبت سن تشريع عام لحماية الخصوصية ، وفضلت اصدار قوانين معينة تحكم قطاعات بعينها ، كما هو الحال بسجلات تأجير الفيديو ، والخصوصية المالية ، وغيرها ، وفي مثل هذه الحالة فان انفاذ القواعد القانونية يتحقق من خلال آليات مختلفة وليس كما هو الحال بالنسبة للقانون الشامل التي ينشئ جهة رقابة عامة . ويؤخذ على هذا النموذج انه يتطلب ان تسنى تشريعات جديدة كلما نشأت تقنيات جديدة ، ولهذا فان الحماية تظل متخلفة عن تقنيات الاعتداء ، وكمثال على ذلك النقص في حقل حماية البيانات المتعلقة بالجينات مثلا ، حيث لا يتم حمايتها بموجب تشريعات الخصوصية حتى الان ، اضافة الى مشكلة عدم وجود الجهة الحكومية المشرفة . وفي كثير من الدول فان القوانين القطاعية تستخدم كقوانين مكملة للتشريع العام بما تتضمنه من تفاصيل اضافية في حقل الحماية لطوائف معينة من المعلومات ، كالاتصالات وسجلات الشرطة وبيانات الاقتراض للعملاء وتشريعات الخصوصية المصرفية او الخصوصية المهنية كما في حقل المحاماة او غيرها .

3 - التنظيم الذاتي SELF - REGULATION ابتداءا لا بد من الاشارة الى ان موضوع التنظيم الذاتي للتشريعات هو موقف بشأن موضوعات تقنيات المعلومات عموما ، وهو النقيض لما يعرف بالتدخل التشريعي لتنظيم موضوعات تقنية المعلومات ، ولكل اتجاه مؤيدوه ومعارضوه ، ايجابياته وسلبياته ، وبالعموم يمكننا القول ان النموذج الامريكي للتعامل مع تقنية المعلومات دعا الى مزيد من تبني فكرة التنظيم الذاتي في حقول التجارة الالكترونية ومعايير الخدمات التقنية وحماية البيانات وأمن المعلومات وغيرها ، مع انه ليس كذلك في حقل الملكية الفكرية مثلا . أما الاتحاد الأوروبي ، فانه يتجه نحو التنظيم الحكومي اكثر، لهذا نجد ان منظماته قد اتجهت دائما الى توجيه دول الاعضاء الى اصدار تشريعات تتلاءم مع القواعد المقررة في الادلة الارشادية والتوجيهية الصادرة عن منظماته كمجلس اوروبا واللجنة الاوروبية والاتحاد الأوروبي ، بل اتجه الى التنظيم التشريعي الشامل عبر قوانين البرلمان الأوروبي .

بين هاذين الرأيين ثمة منطقة رمادية تؤمن بترك كثير من المسائل للتنظيم الذاتي للسوق وجهات الصناعة والانتاج ، لكنها في الوقت ذاته تتدخل لتنظيم مسائل اخرى ، وطبعا كل ذلك وفق الظروف الخاصة بالدولة وتبعا للموضوع محل التنظيم والاستراتيجية الوطنية بشأنه ، فاذا كانت امريكيا مثلا تترك مسألة المعايير والمواصفات التقنية للتنظيم الذاتي للسوق فان هذا الامر مبرر لما يتوفر من قواعد واسعة في حقل منع التنافس غير المشروع وحقل منع الاحتكار وحماية المستهلك وقواعد منع الغش وايهام الجمهور ، في حين ان دولا نامية او حتى متقدمة

لا يتوفر لها مثل هذا الاطار ، لا يكون قرارها بترك تنظيم المعايير للسوق ، بل يتعين التدخل من اجل حماية المستهلك وضمان سلامة الخدمات التقنية الموجهة اليه .

وحماية البيانات يمكن ان تتحقق على الاقل نظريا من خلال اشكال عديدة للتنظيم الذاتي التي ومن خلالها تؤسس الشركات الصناعية والتجارية نظاما خاصا للممارسة وللمعايير ، يعد سياسة ذاتية لها جميعا ، وفي الولايات المتحدة مثلا ، فقد فشلت كثير من جهود التنظيم الذاتي ، ربما بسبب تأثر اهداف التنظيم الذاتي بالمصالح الخاصة الى جانب مشكلة التواؤم مع هذه السياسات وتنفيذها في مختلف الحقول . وفي كثير من الدول فان الكودات الصناعية انتجت حماية ضعيفة مع نقص في القوى التنفيذية ، وتبرز نماذج عديدة من التنظيم الذاتي في كل من اليابان وامريكا وسنغافورة .

وبشكل عام ، يوجد في مختلف التشريعات الوطنية قواعد تحمي السرية (الاطباء ، المحامين ، الوظائف العامة ، التشريعات العسكرية) أما بالنسبة لقوانين حماية البيانات التي نجمت عن استخدام الكمبيوتر فانها تتضمن نصوصا جنائية تتعلق بتخزين البيانات بصورة الكترونية ، وقد تطورت في الاعوام الاخيرة لتشمل عمليات الجمع اليدوي للبيانات ، وتتكامل هذه التشريعات وتكمل بالقواعد المقررة في قوانين حماية البيانات في القطاعات الخاصة ، وبالتالي فان حماية البيانات الشخصية تجد قواعدها في قوانين حماية البيانات وفي تشريعات حماية البيانات في القطاعات الخاصة وكذلك في القواعد العامة المقررة لحماية البيانات في القوانين العامة . وكأثر للتطور التاريخي للحماية فان هناك تباينا واسعا بين النظم الوطنية بشأن الحماية الجنائية لأنشطة جمع المعلومات وتباينا بشأن تحديد الأفعال الجرمية كما سنشير فيما ياتي .

3-4 الغرض من تبني تشريعات شاملة لحماية الخصوصية :-

هناك اسباب رئيسية ثلاثة للتوجه نحو اعتماد نموذج التشريع الشامل للخصوصية وحماية البيانات ، والدول بشكل عام بنت هذه القوانين لسبب او اكثر من بين هذه الاسباب الثلاث : -

1 - تجاوز ومعالجة الانتهاكات السابقة ، فالكثير من الدول وتحديدا في وسط اوروبا وامريكا الجنوبية وجنوب افريقيا تبنت مثل هذه القوانين لمعالجة الاعتداءات التي مارستها السلطات السابقة على الحق في الخصوصية ضمن واقع غياب احترام حقوق الانسان عموما .

2 - تشجيع التجارة الالكترونية وتنظيمها ، فالكثير من الدول ، وخاصة في اسيا ، وضعت مثل هذه القوانين بغرض تشجيع الاعمال والتجارة الالكترونية منطلقة من ان المستهلكين لن يقدموا على التجارة الالكترونية في ظل خشيتهم على بياناتهم الخاصة ، وقد سنت تشريعات الخصوصية كجزء من حزمة تشريعات تهدف الى تسهيل التجارة الالكترونية من خلال مجموعة قواعد موحدة .

3-التأكد من ان القوانين تتلاءم مع المعايير الاوروبية ، فغالبية الدول في وسط وشرق اوروبا تبنت قوانين الخصوصية مستندة الى اتفاقية مجلس اوروبا ودليل حماية البيانات المقر من قبل الاتحاد الأوروبي ، اذ ان غالبية هذه الدول ترغب بالانضمام للاتحاد الأوروبي في المستقبل ، وتعلم ان ذلك يتطلب الانسجام مع ما يقرره الاتحاد والبرلمان الاوروبيين من قوانين ، وكذلك فان عددا من الدول خارج اوروبا تبنت مثل هذه القوانين لان المعايير الاوروبية تمنع تبادل البيانات خارج الحدود مع دول لا تحمي الخصوصية ، او لرغبة بعض الدول التي لها مصالح مباشرة مع الدول الاوروبية للانسجام مع الانظمة القانونية الاوروبية ، كما هو الحال بالنسبة لكندا واستراليا.

4-4 اطار حماية الخصوصية في الدول الاوروبية

في عامي 1995 و 1997 ، سن الاتحاد الأوروبي دليلين إرشاديين من اجل تحقيق الانسجام والتناسق بين قواعد حماية الخصوصية في دول الاتحاد الأوروبي ، ولتوفير مستوى معين بالنسبة لحماية المواطنين الاوروبيين والسماح بالتدفق الحر للبيانات الشخصية داخل نطاق الاتحاد الأوروبي .

وقد قرر هذان الدليلان مستوى معين لحماية الخصوصية لا يقف فقط عند حد حماية البيانات وفق مفاهيم القوانين القائمة حاليا ، ولكن يتجاوزه الى تأسيس مزيد من الحقوق وتوسيع نطاق الحق ذاته .

فبالنسبة الى دليل حماية البيانات لعام 1995 فقد اهتم بمسألة توجيه القوانين الوطنية لتنظيم معالجة البيانات الشخصية بالشكلين الالكتروني واليدوي ، اما دليل الاتصالات لعام 1997 اسس وقرر حماية خاصة تغطي الهاتف والتلفزيون الرقمي وشبكات الهاتف الخلوي وغيرها من نظم الاتصالات ، وكل دول من دول الاتحاد الأوروبي يتعين عليها ان تسن تشريعات ملزمة حتى نهاية عام 98 سندا لهذا الدليل وحتى صيف عام 2000 فان عددا من الدول لم تقم بسن هذه التشريعات بعد .

وسندا للقواعد المقررة في هذين الدليلين ، فان المبادئ الرئيسية لحماية البيانات تتمثل بما يلي : -

1 - الحق في معرفة اين تتم معالجة البيانات

2 - الحق في الوصول الى هذه البيانات وتصحيحها

3 - الحق في الدفاع والحماية من انشطة المعالجة غير القانونية

4 - الحق بالحصول على اذن لاستخدام البيانات في بعض الظروف والاغراض ، فعلى سبيل المثال فان للافراد الحق في الحصول دون مقابل على المعلومات المتعلقة بالتسويق .

ويتضمن دليل حماية البيانات الاوروبي لعام 1995 ، حماية فاعلة ضد استخدام البيانات الشخصية الحساسة ، كالبيانات المتعلقة بالصحة والامور المالية للشخص ، وتلتزم الجهات التجارية والحكومية لدى استخدامها هذه البيانات بالتقيد بقواعد استخدامها ، وبما قرره الدليل للشخص من حقوق عليها ، ذلك ان جوهر مفهـوم حماية البيانات في النموذج الأوروبي هو (فعالية تطبيق قواعد الحماية - التنفيذ) فالاتحاد الأوروبي يهتم بالالية التي يمكن من خلالها ضمان توفير الحماية وانفاذ مبادئها ، ومرد ذلك المشكلات التي ظهرت جراء قدرة الجهات الخاصة والحكومية على الوصول للبيانات من هنا اوجب التوجه الأوروبي وجود جهة رقابة او اشراف تكفل تنفيذ القانون في هذا الميدان ، هذه الجهة تعرف في بعض الدول بالمفوض وفي اخرى بالمراقب وفي ثالثة بمسجل البيانات ، وبغير ذلك من التسميات .

ويفرض الدليل على الدول الاعضاء التزامات بشأن التأكد من ان البيانات الشخصية التي ترتبط بالمواطنين الاوروبين تحظى بنفس المستوى من الحماية عند نقلها الى خارج الحدود او معالجتها بأنظمة معلومات خارجها ويحظر الدليل نقل البيانات الى الدول التي لا توفر قوانينها حماية للخصوصية .

أما بالنسبة لدليل الاتصالات لعام 1997 فانه يفرض التزامات واسعة على جهات خدمة الاتصالات وتزويدها لضمان خصوصية المستخدمين بما في ذلك الانشطة المتصلة بالانترنت ، ويتضمن قواعد تغطي العديد من المسائل التي لم يتم تغطيتها في قوانين حماية البيانات القائمة، ويتضمن القواعد التي تتعلق بتزويد الخدمات التقنية ومسائل الاشتراكات والتعرف على المشتركين وغيرها من المسائل التي نشأت بسبب ثورة الاتصالات . وفي تموز 2000 اصدرت المفوضية الاوروبية نموذجا جديدا لدليل معالجة البيانات الشخصية وحماية الخصوصية في قطاع الاتصالات الالكترونية ، وقد قدم هذا الدليل كجزء من حزمة واسعة تهدف الى تقوية المنافسة في سوق الاتصالات الالكترونية ، ويتعين ان يحل محل دليل الاتصالات لعام 1997 . والدليل الجديد يوسع من نطاق الحماية للافراد ، ويتضمن قواعد بشأن التقنيات الحديثة وطوائفها الجديدة ، كما يتضمن تعريفات جديدة لخدمات الاتصال والشبكات ، وكذلك يضيف تعريفات جديدة للمراسلات والبيانات المنقولة والمكالمات وموقع البيانات وغيرها ، كل ذلك بقصد توسيع نطاق حماية الخصوصية والسيطرة على كافة انواع البيانات المعالجة .

وتؤكد النصوص الجديدة حماية البيانات المنقولة عبر الانترنت وتمنع السلوكيات الاتصالية الضارة في السوق التجاري الالكتروني مثل(SPAM) (رسائل البريد الالكتروني الموجهة دون رغبة المتلقي وباعداد كبيرة وعلى نحو دوري احيانا) وحماية مستخدمي الهواتف الخلوية من الرقابة والمتابعة المتصلة بالموقع ، كما يقدم الدليل وصفا لكافة خدمات الاتصالات الالكترونية كالاتصالات الخلوية والبريد الالكتروني ، والحق بالاختيار بشأن الخدمات المعروضة .

وتجدر الاشارة في هذا المقام ان التوجيهات الصادرة عن الاتحاد الأوروبي عموما تجيز للدول الاعضاء تقييد وتضيق الاحكام بالاستناد الى القواعد المقررة بشأن انفاذ العدالة وتطبيق القانون كلما كان من الممكن حصول التناقض بين ما تقرره الأدلة التوجيهية وبين قواعد رئيسة في النظام العام .

5-4 الاطار العام لتشريعات الخصوصية المعلوماتية .

كما اسلفنا ، فان الخصوصية احد حقوق الانسان الرئيسية التي تتعلق بكرامة الانسان وبقيم مادية ومعنوية اخرى ، كالحق في الرأي والحق في التعبير والمشاركة السياسية ، وقد اصبح الحق في الخصوصية واحدا من اهم حقوق الانسان في العصر الحديث . وجرى الاعتراف بالخصوصية ضمن ثقافات ونظم غالبية الدول ، فجرى حمايتها في الاعلان العالمي لحقوق الانسان وفي العهد الدولي للحقوق المدنية والسياسية ، وفي غالبية اتفاقيات حقوق الانسان الدولية والاقليمية ، وتقريبا فان كل دولة في العالم ضمنت دستورها حكما ما بشأن الخصوصية ، في حدها الادنى فان غالبية النصوص تحمي الحق في حرمة المسكن وسرية الاتصالات (المفهوم المادي للخصوصية) ، ومعظم الدساتير الحديثة تتضمن نصوصا خاصة تعترف بالحق في الوصول والسيطرة على المعلومات الشخصية (البعد المعنوي للخصوصة) ، وحتى في الدول التي لم تتضمن دساتيرها او قوانينها اعترافا بالخصوصية فان المحاكم فيها قد اقرت هذا الحق بشكل او اخر او استنادا الى الاتفاقيات الدولية التي اعترفت بهذا الحق حيثما تكون الدولة عضوا فيها . كما يلحظ ان غالبية الدساتير الحديثة قد تضمنت نصوصا صريحة

بشأن حماية الخصوصية ببعديها المادي والمعنوي ، وان عددا منها تضمن نصوصا بشأن حماية الحق في البيانات الشخصية ، الوصول اليها وادارتها . 6

وقد اظهرت الدراسة البحثية ان نحو 50 دولة من دول العالم قد اقرت تشريعات شاملة في حقل حماية البيانات (Data Protection) وأن نحو 20 دولة تبذل جهودا تشريعية في هذا الوقت لوضع قوانين في ذات الحقل او تعديل قواعدها القانونية القائمة لتحقق حماية البيانات وتحديدا البيانات الشخصية والاسرار من مخاطر المعالجة الالية للبيانات ، وينسب هذا النشاط التشريعي المحموم ، الذي بدء يظهر بشكل ملحوظ في اخر سنتين، الى عوامل عديدة ، منها :- رغبة الكثير من الدول التواؤم مع متطلبات عصر المعلومات ، وخشيتها من المخاطر المتزايدة لوسائل معالجة ونقل البيانات ، الى جانب عامل حاسم اخر هو الرغبة العامة في تشجيع وتنظيم التجارة الالكترونية والتي يعد من بين موضوعاتها الساخنة مسائل الخصوصية ، ورغبة هذه الدول ايضا - واحيانا اضطرارها - للتواؤم مع توجهات المنظمات والهيئات الدولية او متطلباتها سواء الهيئات التي تكون الدولة عضوا فيها او تلك التي ترتبط مع دولها بمصالح والتزامات توجب عليها انفاذ استراتيجياتها وسياساتها التوجيهية ، كالدول التي وجب عليها تحقيق المعايير المقررة في حقل تبادل البيانات عبر الحدود المقررة من قبل الاتحاد الأوروبي ومجلس اوروبا ومنظمة التعاون الاقتصادي والتنمية .

لقد تم سن تشريعات خاصة ضد انشطة الاعتداء على الخصوصية في مختلف النظم القانونية الغربية مع تباين طفيف بينها ، وقد تبنت المحاكم في غالبية هذه الدول قواعد طورت من نطاق الحماية في حقل اقرار احكام التعويض عن الضرر . والتحليل المقارن للقوانين الوطنية اظهر ان العديد من المنجزات العالمية قد تحققت في حقل توحيد التنظيم الاداري والقانوني لحماية الخصوصية في القوانين الوطنية ، فغالبية القوانين الوطنية لحماية البيانات تتضمن على سبيل المثال نصوصا تقيد عملية جمع البيانات وتسمح للافراد بالوصول اليها ، وتقر المبادئ التي تمثل الحد الادنى المشار اليها فيما تقدم ، لكن هذا الانسجام لا يمنع من وجود فوارق بين هذه التشريعات اهمها تلك المتعلقة بنطاق التطبيق (ما اذا كانت الحماية تشمل بيانات الاشخاص الطبيعيين فقط ام تمتد للاشخاص المعنويين، وما اذا كانت تشمل البيانات المؤتمتة فقط ام تمتد للبيانات اليدوية) وكذلك الاحكام المتعلقة بالقواعد الاجرائية المتطلبة لعمليات جمع ومعالجة ونقل البيانات والجهات المناط بها السيطرة والاشراف والرقابة على الانشطة المتعلقة بالمعالجة الالية للبيانات . والخلاف لا يتوقف على هذه الابعاد الادارية والتنظيمة ، بل يمتد ايضا وبشكل اوسع الى مسألة تحديد الأفعال الجرمية وكذلك تحديد العقوبات المقررة على الأفعال الجرمية التي تعد اعتداءا على حماية البيانات الشخصية واوسع اوجه الخلاف في حقل الحماية الجنائية يظهر في تحديد المحظورات وبيان الاستثناءات المشروعة على هذه المحظورات .

ففي حقل ما يمكن تسميته جرائم الخصوصية المعلوماتية ، فان الخلاف بين تشريعات الخصوصية المشار اليها اعلاه يكمن بتحديد الأفعال غير القانونية محل التجريم ، ففي بعض الدول كالولايات المتحدة واليابان لا يستخدم القانون الجزائي لحماية الخصوصية بشكل عام ، وهذا هو حال القانون الامريكي التي لا يتضمن سوى افعال جرمية محدودة ، وكذلك تشريعات الخصوصية في كندا التي لا تنص سوى على فعل جرمي واحد في ميدان حماية الخصوصية ، وفي القانون الياباني لا يجرم الا الحصول على البيانات الشخصية من جهات ادارية ، وشبيه بها قانون حماية البيانات الهولندي الذي يعاقب فقط على الاخلال بتسجيل ملفات البيانات . وعلى العكس بذلك نجد العديد من الدول تتضمن قائمة تفصيلية للافعال الجرمية التي ترجع الى الكثير من الانشطة المحظورة من قبل الجهات الادارية او الاشخاص ، واوضح مثال على هذه التشريعات القانون الفرنسي التي حدد كافة الانماط الجرمية التي تستهدف الخصوصية تبعا لمراحل الجمع والمعالجة والتبادل التي تتم على البيانات .

فالتشريع الفرنسي التقليدي كان قد جرم التعدي على الأمور التي تدخل في نطاق الحياة الخاصة ، كالأمور التي تتعلق بالشرف والاعتبار وحرمة المسكن والمراسلات والمحادثات . أما الفقه الفرنسي ، فقد حاول وضع قائمة بالحالات أو الأمور التي تتعلق بالحياة الخاصة للأفراد وتبني القضاء الفرنسي ما ذهب اليه جانب من هذا الفقه . وكأثر لجدل قضائي وفقهي تم سن تشريع خاص بحماية جمع ومعالجة البيانات الشخصية وتجريم مختلف صور الاعتداء عليها سواء من قبل القائمين على عمليات الجمع ام من قبل الغير .

أما بالنسبة لنطاق الخصوصية في النظام الأمريكي ، فقد حدده بالأساس الفقيه الأمريكي بروسر Prosser - وتبنى هذا التحديد القضاء الأمريكي واعتمده أيضا المشرع الأمريكي في المدونة الثانية الصادرة عام 1977 بشان الخصوصية .

ويشمل نطاق الحق في الحياة الخاصة أو (الخصوصية) في النظام الأمريكي ، حماية الأفراد من أربع صور رئيسية للاعتداء على الخصوصية:-

التدخل في الحياة الخاصة للفرد (حق الفرد في العزلة)

استخدام اسم أو صفة الغير دون رضاه .

إفشاء أسرار الحياة الخاصة للغير .

الإساءة الى سمعة الشخص في نظر الجمهور كاستخدام اسمه على نحو يسيء لسمعته دون إذنه .

---

6 انظر الدول التي تضمنت دساتيرها نصوصا تتعلق بالخصوصية ضمن قائمة التشريعات فيما ياتي من هذا الفصل ، وانظر النصوص التي وردت في هذه الدساتير في العديد من مواقع القانون على الانترنت التي تتضمن دساتير العالم ومنها :- http://www.uni-wuerzburg.de/law/index.html وكذلك موقع الخصوصية العالمي المشار اليه فيما تقدم :- www.internationalprivacy.org.

ان توفير الأداة القانونية لمواجهة أخطار المعالجة الآلية للبيانات الشخصية قد انطلق كما اسلفنا مع مطلع السبعينات ، وقد قادت دولة السويد الطريق بتشريع خصوصية البيانات ، وتبعتها الولايات المتحدة الأمريكية بقانون الخصوصية عام 1974 والذي أسس للمبادئ العامة ، ويؤكد قانون الخصوصية الأمريكي لعام 1984 الذي يعتبر أقوى بكثير من سابقه على إعلام الأفراد بان سجلات شخصية يتم جمعها عنهم وحفظها ، ويعطيهم الحق ليشاهدوها ويصححوها ويمنع من استخدام المعلومات التي تم تزويدها في أي غرض آخر غير التي زودت من اجله . وفي المملكة المتحدة ، فقد تم إقرار قانون حماية البيانات عام 1984 والذي فرض على كل التنظيمات التي لديها معلومات عن الأفراد على حواسيبها تسجيل نوع البيانات التي لديهم من خلال مسجل حماية البيانات ، ويمكن القانون المواطنين من الحصول على تعويض من خلال المحاكم الدينية إذا ما وجد أن البيانات الشخصية التي لديهم ليست دقيقة أو إذا ما ضاع هذا السجل أو تم الإفصاح عنه الى شخص غير مصرح له .وقد وضع المشرع في ألمانيا الغربية عام 1986 قانون حماية البيانات (القانون المعدل لقانون 1977) متزامنا مع إقرار قانون يصرح باستخدام بطاقات التعريف التي يتم قراءتها بواسطة الحاسوب ، ويفرض على كل الألمان الغربيين أن يحملوا بطاقات (ID) الجديدة مما يسمح للسلطات خزن البيانات عن حركة الناس على حواسيب مركزية . وهو ما لقي معارضة صلبة من الكثيرين ، بما فيهم موظفو حماية البيانات في الحكومات الإقليمية ، لمحاربة استخدام هذه البطاقات لمساسها بالحقوق الشخصية .

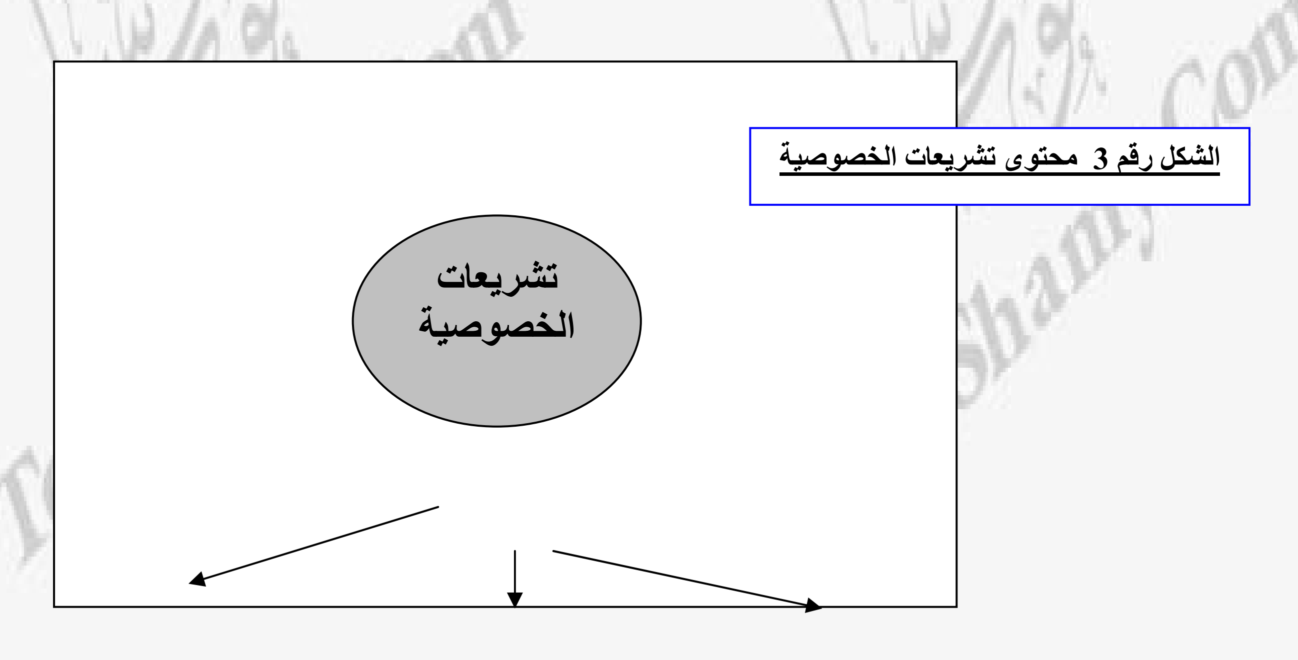
وقد تأثرت على نحو آخر العديد من الدول ، بتشريعات كل من فرنسا وأمريكا وألمانيا والسويد في مجال التنظيم القانوني لحماية الحياة الخاصة . وجاء نشاط المنظمات الدولية والإقليمية المتقدم عرضه ، وعلى نحو خاص ، المنظمات الأوروبية ، ليؤطر من جهة ، جهود حماية البيانات الشخصية والحق في الحياة الخاصة ، وليخلق اتساقا عاما بين قواعد التشريعات الوطنية لمختلف الدول التي سنت قوانين لحماية الخصوصية أو الحياة الخاصة ، فمثلت مبادئ القواعد الإرشادية لمنظمة التعاون الاقتصادي والتنمية ، واتفاقية مجلس أوروبا وقرارات وتوصيات السوق الأوروبية المشتركة ، والمبادئ التوجيهية المتعلقة باستخدام ملفات الأشخاص المعالجة آليا التي أعدتها اللجنة الفرعية لمنع التمييز وحماية الاقليات (هيئة تابعة للمجلس الاقتصادي والإجماعي في هيئة الأمم المتحدة) ، مثلت إطارا - في حده الأدنى - لكفالة اتساق وتطابق قواعد الحماية الخاصة والمعالجة الآلية للبيانات الشخصية .

من هذا الاستعراض الموجز والمكثف ، فان قوانين الخصوصية تنطوي على ثلاث طوائف رئيسة من القواعد :-

الاولى :- الطائفة المتعلقة باقرار المباديء الرئيسة للحق في الخصوصية ونطاق اعتراف الدولة به وكفلته والالتزامات المقررة على الجهات العامة والخاصة في حقل حماية البيانات الشخصية واحترام الخصوصية فيما تمارسه من انشطة جمع ومعالجة البيانات الشخصية باستخدام التقنية.

الثانية :- القواعد التنظيمية والاجرائية والمعايير ، وهي تلك القواعد المتعلقة باليات جمع البيانات ومعالجتها ونقلها وتحدد المعايير التي يتعين على جهات التقنية والاتصالات التقيد بها الى جانب بحثها في جهات رقابة حماية الخصوصية وتنظيم تشكيلها وعملها وبيان دورها وتحديد مهامها وصلاحياتها يضاف اليها ايضا القواعد الاجرائية الخاصة التي تطبق بالنسبة للحماية المدنية او الجزائية المقررة في نطاق القواعد الموضوعية للحماية .

الثالثة :- القواعد الموضوعية للحماية المدنية والجنائية ، وتشمل نصوص التجريم مع تحديد للافعال المجرمة وعقوباتها ، اضافة لبيان نطاق المسؤولية المدنية ، وبيان الجهات محل المساءلة وغير ذلك من قواعد موضوعية تتعلق بالحماية القانونية للبيانات الشخصية في كافة مراحل التعامل التقني معها . ويوضح الشكل 3 تاليا الاطار العام لمحتوى تشريعات الخصوصية كما يوضح الجدول رقم 1 السمات العامة لتشريعات حماية الخصوصية .



الشكل رقم 3 محتوى تشريعات الخصوصية

نطاق الاعتراف بالحق وقواعد كفالته وحمايته	القواعد التنظيمية والاجرائية والمعايير	قواعد الحماية الموضوعية المدنية والجزائية

جدول رقم 1

(جدول 1 خصائص ومحتوى تشريعات حماية الخصوصية)

مسماها الشائع	قوانين الخصوصية Privacy او قوانين حماية المعطيات Data Protection laws .
وصفها العام	تشريعات حماية الحياة الخاصة من مخاطر المعالجة الإلكترونية للبيانات الشخصية.
مبرر وجودها	هذه التشريعات جاءت كرد فعل للتحديات التي واجهتها الحياة الخاصة بسبب مخاطر المعالجة الالية للبيانات الشخصية وازدياد انشطة جمع (Collecting) وتخزين (Storing) وتبادل ونقل البيانات (Transmitting data) بالتقنيات الحديثة .
هدفها ونطاقها	سنت هذه القوانين لحماية حق المواطنين في الخصوصية وحماية بياناتهم الخاصة واسرارهم ضمن قواعد ادارية ومدنية وجزائية.
الحقبة الزمنية لانطلاقها وترتيبها بين موجات تشريعات التقنية	في عام 1968 وعلى اثر عقد مؤتمر الامم المتحدة (طهران) لحقوق الانسان ومناقشة موضوع مخاطر تكنولوجيا المعلومات على الحق في الخصوصية ظهرت هذه التشريعات كـأول موجة تشريعية وقد انطلقت خلال السبعينات والثمانينات . وخضعت لتعديلات متتالية خلال الثمانينات والتسعينات .
الفرع القانوني ذو العلاقة	حقوق الانسان (تحديدا الحق في الحياة الخاصة) ، والقانون الجنائي (المسؤولية الجزائية عن الاخلال بواجبات المعالجة وعن افشاء البيانات) ، القانون الاداري (انظمة التنظيم الاداري ، وقواعد نقل تبادل المعلومات بين الهيئات الحكومية) .
محلها ذو العلاقة بالتكنولوجيا	البيانات الشخصية المخزنة والمعالجة والمتبادلة بواسطة الكمبيوتر وشبكات نقل المعلومات (بما فيها وفي مقدمتها الانترنت).
محتواها بوجه عام	القواعد القانونية المنظمة لمعالجة البيانات وتخزينها في بنوك المعلومات وتبادلها وتشمل القواعد التي تحظر جمع المعلومات دون سند قانوني وتوجب جمعها للغرض المعلن واستخدامها في هذا الغرض وحده ، وتتيح الحق في تصحيحها وتعديلها من اصحابها ، ولا تجيز إفشاءها وتقرر عقوبات على القائمين بالمعالجة والتحكم في هذه البيانات عند الاخلال بواجباتهم وتقييم المسؤولية على التوصل اليها من الاشخاص الخارجين عن المؤسسة المعنية بالجمع والمعالجة والمسؤولية عن افشائها او الابتزاز بواسطتها .

5- امن المعلومات والجرائم التقنية – الماهية والمخاطر واحتياجات حماية الاعمال الالكترونية اللاسلكية .

1-5 ماهية جرائم التقنية ومخاطرها

مفهوم جرائم التقنية العالية او جرائم الكمبيوتر ، مفهوم مستحدث على الصعيد العالمي، فبالرغم من ان اول حادثة موثقة لاساءة استخدام الكمبيوتر ترجع الى عام 1959 ، فان التشريعات التي وضعت لمواجهة خطر جرائم الكمبيوتر تأخرت حتى اواخر السبعينات مطلع الثمانينات (وتوصف بأنها موجة التشريع الثانية لتقنية المعلومات وانها موجة الثمانينات مع ان ثمة انطلاق لقوانين جرائم الكمبيوتر في مطلع السبعينات كما تقدم) وبقيت في حدود ضيقة وفي اطار عدد محدد من الدول والاهم من ذلك بقي نطاق الحماية من جرائم الكمبيوتر حتى الوقت الحاضر قاصرا عن الاحاطة بكل جرائم الكمبيوتر كما سنرى فيما يأتي .

احداث كثيرة نسمعها وتتناقلها وسائل الاعلام [7] عن انواع فريدة من جرائم الكمبيوتر ، وربما يعتقد البعض انها حديثة وربما سبب ذلك ترافق الحديث الواسع عن هذه الظاهرة مع شيوع الانترنت وتطور هجمات مخترقي النظم ، الى مدى اختلطت فيه المفاهيم فاصبح البعض يقتصر ادراكه بشان جرائم الكمبيوتر على انشطة (الهاكرز) ، أي مخترقي مواقع المعلومات ونظمه عبر الانترنت . لكن حقيقة حوادث اجرام التقنية يرجع الى الستينات والسبعينات ، وقد اتخذت اشكالا عديدة وانماطا عديدة وتطورت انماطها خلال الثمانينات والتسعينات ، لكنها بالتاكيد تشمل كل هذه الانماط ولا تقف عند انماط الاختراقات في بيئة الانترنت .

ان خط الحدث الجرمي في عالم التقنية زاخر بالانشطة غير المشروعة ، فمن استغلال مبرمج في احد المصارف سيطرته على نظام مالي ما بحيث يقوم بزرع اوامر تتيح له تحويل مبالغ من حسابات الزبائن الى حساب عائد له او لأحد شركائه في الجرم تمهيدا للاستيلاء على المال ، كما حدث في مطلع السبعينات في السويد والمانيا وسويسرا وغيرها ، الى الدخول دون تصريح او تخويل الى احد النظم والعبث بالبيانات والمعلومات المخزنة فيه ، تغييرها او تحويرها او انشاء معلومات وهمية او اعادة توجيهها الى هدف غير المرسلة اليه ، او حتى تدميرها ، ومثالها آلاف الانشطة الجرمية باستخدام برامج التخفي واعتراض البيانات والفيروسات والديدان الالكترونية والاختراقات غير القانونية اعتبارا من مطلع الثمانينات وحتى الان ، والتي كانت في اشكالها الاولى تتم بتوسل الدخول الى نظام مغلق او من خلال الدخول الى الشبكات الخاصة عن بعد ، فأتاحت الان الانترنت قدرة الدخول عن بعد ولآلاف الاجهزة وقواعد البيانات .

ومن انشطة تعطيل الانظمة بالبرمجيات الخبيثة او حتى التدمير المادي لها او استغلالها دون تصريح ، الى انشطة الهجمات عبر الانترنت على مواقع المعلوماتية لجهة تعطيل عملها فيما يعرف بهجمات انكار الخدمة باستخدام تكنيك بث آلاف الرسائل الالكترونية دفعة وحدة او باستخدام القنابل الموقوتة او المنطقة او الفيروسات او غيرها كما حدث في العام الماضي (2000) فيما يعرف بظاهرة تعطيل عمل اشهر مواقع الانترنت .

اذن ، ثمة اكثر من مجرد شخص يتوسل الهجوم على موقع انترنت من الخارج ، وربما يكون ذلك اسهل الشرور ، فجرائم الكمبيوتر شملت انشطة التجسس الصناعي والامني ، الاستيلاء على البيانات والمعلومات ذات القيمة الاقتصادية او التي تمثل قيما مالية كالقيود المصرفية ، اجراء تحويلات وهمية للنقود ، تدمير المعطيات وتشويها او اصطناع بيانات ووثائق الكترونية وهمية ، الاستيلاء على ارقام بطاقات الائتمان واستخدامها بشكل غير مشروع للاستيلاء على المال ، الاساءة لسمعة الافراء وتحقيرهم عبر نسبة رسائل الكترونية لهم ، استغلال مواقع الانترنت في ترويج محتوى غير قانوني او في ادارة نشاط غير قانوني كالقمار ودعارة الاطفال .

انها انشطة لا تقتصر على مجرمين عتاة يقارفون انشطتهم من الخارج، بل اخطرها ما يمارس من قبل موظفي المنشأة ذاتها ، أي من الداخل وليس من اشخاص يتوسلون اجتيازا غير مشروع واختراقا لنظم المعلومات من خارج المنشأة . وبالمفاهيم التقليدية للافعال - التي تختلف كما سنرى عن السلوكيات المقررة في نصوص التجريم القائمة - فان جرائم الكمبيوتر تمتد لتغطي السرقة ، الاختلاس ، التزوير ، الاحتيال ، الاتلاف والتدمير ، الافتراء ، تعطيل الخدمة ، الاستغلال غير المشروع للمال ، الاضرار بمال الغير .. الخ من الافعال التي ربما تصل حد القتل .

---

[7] وبالمناسبة تساهم وسائل الاعلام كثيرا في تشويه الحدث او في عدم سلامة التعاطي مع نطاقه الحقيقي .

ان احد اشهر قضايا الاختراق تضمنت في نهاية الثمانينات مجموعة من المراهقين الالمان الذين تمكنو من الدخول الى انظمة العديد من الشركات الامريكية وجمع معلوماتها بقصد بيعها الى المخابرات السوفيتية (سابقا) وقد اكتشفت هذه القضية عن طريق تعاون احد (الهكرز) مع جهات التحقيق بحيث قدم لها كافة معلوماته بشأن كيفية حدوث الاختراقات والانظمة المستهدفة ، وقد كانت هذه القضية من اكثر القضايا اهمية بالنسبة لجهات التحقيق فيما بعد ، لما كشفته من تفاصيل عن الاليات التقنية والوسائل التي استخدمها هؤلاء الهكرز في الحصول على المعلومات .

ويعتمد تكنيك الاختراق (هاكنج Hacking) بشكل اساسي على طبيعة الاتصال بالنظام ووسائل الاتصالات المرتبطة بنظام الكمبيوتر ، وتعتمد انشطة الهكرز التقليدية (في طورها البدائي) على تجاوز كلمات السر التي تحمي انظمة الكمبيوتر ، وقد كانت تتم عن طريق تخمين الكلمة تبعا للشخص المستخدم او المؤسسة ، سيما وان غالبية كلمات السر تكون مرتبطة بحوادث ووقائع واسماء مألوفة ومتصلة بشخص مستخدمها (تاريخ الميلاد ، اسم الزوجة ، اسم الصديق او الصديقة ، اسم المنشأة ...... الخ) وقد تطور اسلوب الحصول على كلمات السر عن طريق استخدام برمجيات الاحتمالات وربطها بالنظام المنوي اختراقه . ومع شيوع استخدام الانترنت والربط الواسع للشبكات المحلية بالشبكة العالمية فان اساليب الهكرز قد تغيرت، اذ اصبحو يعتمدون على عمليات الدخول عن طريق الشبكة واستغلال برتوكولات الاتصالات المستخدمة فيها او وسائل تقصي البيانات الخاصة بالمستخدمين مثل (web spoofing) بعد جمعها وتحليلها اونسخ كلمات السر الخاصة بهم ، وكذلك عن طريق اعتراض البيانات وانشاء نظم وهمية للاستقبال والتوجيه تلتقط الرسائل وعناوين المواقع وتتظاهر بأنها الجهة المرسلة اليها ، بل انهم طوروا وسائل لتجاوز كافة اجراءات الامن ، كتجاوز جدران النار وفك شيفرات التشفير وتجاوز بروتوكولات امن البريد الالكتروني ، وغير ذلك من وسائل تقنية .

وفي مرحلة تطور الاتصالات الحالية ، فان انشطة الهكرز امتدت بشكل كبير الى نظم الهاتف والاتصالات ، واصبح نشاطهم لا يستهدف انظمة الكمبيوتر فقط ، بل تزايدت انشطة الاختراق لخطوط الهاتف والة تسجيل الهاتف ونظام البريد الصوتي وغيرها ، وشاع مؤخرا اصطلاح هكرز الهاتف الى جانب هكرز الكمبيوتر ، ويتبع الهكرز في حقل الاتصالات العديد من الوسائل الالكترونية وربما بعضها وسائل مادية الى جانب الوسائل الالكترونية من اجل استراق السمع والتقاط الاتصالات وتحويل سير البيانات والاستيلاء عليها .

ومن امثلة جرائم الهكرز التي تستهدف الهواتف حادثة وقعت عام 1992 عندما تمكن احد الشباب الالمان حديثي السن من اختراق نظام الكمبيوتر الناطق لبنك (بريكلز في هامبرج) والذي يتم فيه تزويد البنك بارقام بطاقات الائتمان وبطاقات البنك الخاصة بالزبائن ، وأيضا تسليم النظام رقم التعريف الشخصي ، وكذلك الارقام السرية اللازمة لاستجابة النظام ، وقد تم من قبل هذا المخترق جمع العديد من المعلومات عن زبائن البنوك والحصول على مثل هذه الارقام .

وربما كانت انشطة التجسس الامني فيما مضى ، وتحديدا في حقبة الحرب الباردة اكثر الانشطة التي تستهدف قواعد المعلومات السرية ايا كان شكل تخزينها ، آليا ام يدويا ، لكن التجسس الذي بدا فيه الكمبيوتر وسيلة خطرة للحصول على المعلومات في الفترة الاخيرة ، يتمثل في الحقيقة بالتجسس الصناعي . فكثير من الشركات المتنافسة في ميدان الصناعة والخدمات تسعى الى الحصول على معلومات سرية واسرار صناعية وتجارية عن خصومها من الشركات بقصد محاولة تحقيق منافع او تقوية مركزها في السوق ، ولم تعد فكرة زرع موظف لاحدى الشركات في شركة منافسة الوسيلة الامثل لما تنطوي عليه من احتمالات الفشل في كثير من الاحيان بسبب استراتيجيات الصلاحيات الوظيفية والمعلومات المصرح كشفها للموظفين تبعا لوظائفهم ومراتبهم ، الى جانب خطورة احتمالات الكشف وتعريض الشركة للمسؤولية ، من هنا كان استخدام وسائل اختراق نظم الكمبيوتر الاكثر فعالية لانجاز التجسس الصناعي ، خاصة ان حجم الاسرار التجارية والصناعية والمعلومات المتعلقة بالاداء والانتاج والتسويق وحتى شؤون الموظفين تجد مكانها داخل ملفات ونظم الكمبيوتر ، والحصول عليها يعدو امرا في غاية السهولة اذا امكن الدخول الى النظام الذي يحتوي هذه المعلومات . وتجدر الاشارة هنا ان الحديث عن التجسس الصناعي يتعلق بوسائل التجسس للكشف عن الاسرار التجارية وليس عملية الاستيلاء على سر تجاري ما ضمن المفهوم الذي يتضمنه قوانين الاسرار التجارية في حقل الملكية الفكرية .

ومن اشهر دعاوى التجسس الصناعي حادثة الاستيلاء على المعلومات المرسلة الى شركة سيمنس الالمانية من قبل احدى شركات الصناعية الفرنسية والمتعلقة بعروض تنفيذ شبكة القطارات السريعة في كوريا الجنوبية ومن الحوادث التي حصلت مؤخرا واقعة تجسس شهيرة بين شركتي طيران عالمتين (البوينغ وايربص) .

والإنترنت أو بالمفهوم المتناقل حاليا (سايبرسبيس Cyberspace) لدى غالبية خبراء التقنية بيئة غير آمنة اذا تخلفت وسائل الحماية التقنية وغابت ادوات الحماية القانونية 8، وقد مثلت الانترنت بالنسبة للعديد من المجرمين ، المكان الذي يمكن فيه تدمير سمعة الشخص أو العمل ، فمجرد خبر عبر موقع ويب (web site) أو من خلال المجموعات الإخبارية (News Group)9 يمكن أن يحدث ضررا كبيرا ، وذلك بسبب الانتشار الواسع للخبر بفعل مميزات شبكة الإنترنت وسرعة انتقال المعلومات عبرها . ان القانون لايمكنه أن يقف صامتا أمام الضرر الذي تحدثه أنشطة الافتراء وإساءة السمعة Defamation عبر موقع الانترنت (الويب سايت) والبريد الإلكتروني ومجموعات الأخبار ، ويتعين ان تنشأ مسؤوليات قانونية عن هذه الأفعال تعرض مرتكبيها للمقاضاة كي لا يبقى الاعتقاد السائد لدى ممارسي هذه الأنشطة انه لا مسؤولية على أفعالهم المرتكبة عبر الخط On line 10.

ان الانترنت وفقا لدراسات الامن المعلوماتي تتعرض في هذه المرحلة - من ضمن ما تتعرض له - الى خطر هجمات انكار الخدمة التي تستهدف ام مواقع المعلومات والنشاط الاستثماري ، وهجمات انكار الخدمة 11باتت النشاط الابرزفيما يعرف بحرب المعلومات ، اذ لم تقف هذه الحرب عند التجسس المعلوماتي والتجسس الصناعي او الامني ، بل اتجهت الى السيطرة على اتجاهات الخدمة المعلوماتية واظهار المقدرة على التفوق في عالم الانترنت.

واذا كان البريد الإلكتروني افضل شيء حصل في عالم الاتصالات منذ الهاتف ، فان الاستخدام الخاطئ للبريد الإلكتروني من قبل الموظفين قد ينشيء مسؤولية صاحب العمل ، فالبريد الإلكتروني من حيث حقيقته لا يختلف عن الرسالة ، فليس لأنه وسيلة إلكترونية يكون غير ذات قيمة مقارنة بالوسائل التقليدية للاتصال وتبادل المعلومات ، وإذا كان صاحب العمل مسؤولا عن الرسائل التقليدية ، فانه سيكون مسؤولا عن البريد الإلكتروني . وثمة أخطاء قد ترتكب من الموظفين في حقل البريد الإلكتروني تماما كتلك التي ترتكب منهم في بيئة الرسائل الورقية ، فقد يعتدي الموظف على حقوق المؤلف ، أو على الأسرار التجارية ، او يرسل مادة تعرض للمسؤولية ، وقد يلزم الشركة بعقد أو تصرف .

ان مخاطر استخدام البريد الإلكتروني وما يمكنه أن يلحق بالمؤسسات من مسؤوليات لا يستدعي عدم استخدامه ، بل مع العكس ، فان استخدامه في بيئة التراسل حقق مكاسب كثيرة أهمها توفير الكلف المالية ، لكن المطلوب في المقابل ، تنظيم استخدامه ضمن ما يمكن تسميته (سياسة البريد الإلكتروني في العمل) تراعي ترتيبات الاستخدام من جهة ، ومن جهة أخرى تكون مدركة للمخاطر محتاطة لمواجهتها .

والكمبيوتر في حالات معينة قد يكون كابوسا بالنظر الى خطورته في نشر المعلومات ، وتماما كما يلزم الشاهد بتسليم محرر كتابي فانه قد يلزم بإحضار وإظهار قاعدة بيانات مخزنة في الكمبيوتر ، انه من السهل السيطرة على الوثائق عندما تكون بصفتها الورقية اكثر من السيطرة عليها عندما تكون بصفتها الرقمية Computerized ، فبين أشرطة الحفظ Backup Tapes والنسخ Copies والأقراص اللينة Floppy Disks ، وسلة المهملات Recyclebin ، فان البيانات المهملة أو المدمرة Destroyed قد تجد طريقها للخبراء والمنقبين في ملفاتك لكشفها ومعرفتها .

---

8 تشير احصائيات مجموعة غارتنر للابحاث الى حقيقة مفادها ان نسبة تتراوح ما بين 50 الى 75 بالمائة من خادمات ويب " مكشوفة " وان الوضع الامني على الويب غير مستتب البتة طبقا لجون بسكاتور ، مدير قسم ابحاث امن الشبكة ، في غارتنر . اضف الى هذه المعلومة القيمة معلومة اخرى اهم ، وهي ان عدد البرمجيات المجانية المتاحة على الويب والتي يمكن استخدامها في عمليات الاختراق قد نما بشكل كبير . وهذه البرمجيات تجعل من الممكن لاي شخص ان يقوم باجراء مسح تلقائي لمواقع الانترنت والبحث عن نقاط الضعف فيها ، ويشبه ذلك التجول في حي ما وفحص كل بيت فيه بحثا عن نافذة غير موصدة او باب غير مغلق . ويقول بسكاتور ان المواقع التي يتم الهجوم عليها واستغلالها ليست بالضرورة المواقع الكبرى ولا يقتصر الامر عليها ، ويضيف في هذا الصدد بقوله ، بالطبع الشركات الكبرى يتم مهاجمتها اكثر من غيرها ، فموقع مايكروسوفت يهاجم في كل دقيقة من اليوم ولكن باستخدام برمجيات التلصص المؤتمتة فان بامكان العابثين ان يقوموا بمسح كافة مواقع الانترنت بشكل تلقائي بحثا عن الثغرات . وفي حين ان المؤسسات صاحبة هذه المواقع يمكنها الانتباه الى حدوث الاختراق وسد الثغرات بشكل مباشر ، فان البرمجيات المتوفرة الان تزيد بشكل كبير من احتمالية اكتشاف العابثين لهذه الثغرات اولا (الانترنت من الالف الى الياء ص 4) .

9 المجموعات الإخبارية أو مجموعة الأخبار news group هي كالنشرات المتبادلة عبر الكمبيوتر computer bulletin board والتي يمكن للملايين قراءتها عبر البريد الإلكتروني E-mail.

10 ((ان العديد من القائمين على مواقع الانترنت حاليا لا يعلمون انه قد تم اختراقهم الا بعد حصول الحدث . ورغم ان هنالك مجموعة كبيرة من المنتجات والخدمات المتوفرة لزيادة الامن مثل برمجيات اكتشاف الدخلاء INTRUSION DETECTION فان القائمين على الشبكات لا يمكنهم معرفة متى تحدث محاولة لاختراقهم او اذا ما كان ذلك قد حدث ومتى)) ((ومع انتشار مجموعات العابثين على الانترنت وتنوع تخصصاتها فان مستوى الضرر الذي يمكن احداثه زاد بشكل كبير فخلال شهر شباط / فبراير الماضي قام احد العابثين بوضع بيان صحفي مزيف على موقع احدى الشركات الكبرى في الولايات المتحدة عن صفقة وهمية مما ادى الى احدث تغيرات كبيرة في اسعار اسهم هذه الشركة قبل ان يتم اكتشاف الخدعة , وحسب ابحاث مجموعة غارتنر فان عملية اختراق احدة مثل هذه تتيح المجال لعملية احتيال في سوق الاسهم بقيمة 4 ملايين دولار . ويقول بسكاتور ان الانترنت جعلت عمليات الاحتيال اكثر سهولة بتأثير سلبي اكبر)) (الانترنت من الالف الى الياء ص 4)

11 خلال شهر شباط 2000 ، قام مجموعة من العابثين باستخدام اسلوب (هجوم الحرمان من الخدمات) Denial of Service attack وهو اسلوب في التخريب يعتمد على اغراق موقع ما بحزم تأتي آنيا من عدة اجهزة خادمة تم اختراقها واستخدامها لبعث هذه الرسائل . ورغم ان زمن توقف المواقع موضع النقاش عن العمل كان في المتوسط اقل من ساعة واحدة فان الاضرار الناتجة عن هذه الهجمات كانت ضخمة حيث قدرت مجموعة يانكي للابحاث ان المواقع التي تعرضت للهجمات خسرت حوالي 1,2 بليون دولار امريكي (الانترنت من الالف الى الياء ص 10)

2-5 دور الكمبيوتر في الجريمة .

يلعب الكمبيوتر ثلاثة ادوار في ميدان ارتكاب الجرائم ، ودورا رئيسا في حقل اكتشافها ، ففي حقل ارتكاب الجرائم يكون للكمبيوتر الادوار التالية :-

الاول:- قد يكون الكمبيوتر هدفا للجريمة (Target of an offense) ، وذلك كما في حالة الدخول غير المصرح به الى النظام او زراعة الفايروسات لتدمير المعطيات والملفات المخزنة او تعديلها ، وكما في حالة الاستيلاء على البيانات المخزنة او المنقولة عبر النظم .

ومن اوضح المظاهر لاعتبار الكمبيوتر هدفا للجريمة في حقل التصرفات غير القانونية ، عندما تكون السرية (CONFIDENTIALITY) والتكاملية أي السلامة (INTEGRITY) والقدرة أو التوفر (AVAILABILITY) هي التي يتم الاعتداء عليها ، بمعنى ان توجه هجمات الكمبيوتر الى معلومات الكمبيوتر او خدماته بقصد المساس بالسرية او المساس بالسلامة والمحتوى والتكاملية ، او تعطيل القدرة والكفاءة للانظمة للقيام باعمالها ، وهدف هذا النمط الاجرامي هو نظام الكمبيوتر وبشكل خاص المعلومات المخزنة داخله بهدف السيطرة على النظام دون تخويل ودون ان يدفع الشخص مقابل الاستخدام (سرقة خدمات الكمبيوتر ، او وقت الكمبيوتر) او المساس بسلامة المعلومات وتعطيل القدرة لخدمات الكمبيوتر وغالبية هذه الأفعال الجرمية تتضمن ابتداءا الدخول غير المصرح به الى النظام الهدف (UNAUTHORIZED ACCESS) والتي توصف بشكل شائع في هذه الايام بأنشطة الهكرز كناية عن فعل الاختراق (HACKING) .

والافعال التي تتضمن سرقة للمعلومات تتخذ اشكال عديدة معتمدة على الطبيعة التقنية للنظام محل الاعتداء وكذلك على الوسيلة التقنية المتبعة لتحقيق الاعتداء ، فالكمبيوترات مخازن للمعلومات الحساسة كالملفات المتعلقة بالحالة الجنائية والمعلومات العسكرية وخطط التسويق وغيرها وهذه تمثل هدفا للعديد من الجهات بما فيها ايضا جهات التحقيق الجنائي والمنظمات الارهابية وجهات المخابرات والاجهزة الامنية وغيرها ، ولا يتوقف نشاط الاختراق على الملفات والانظمة غير الحكومية بل يمتد الى الانظمة الخاصة التي تتضمن بيانات قيمة ، فعلى سبيل المثال قد يتوصل احد المخترقين للدخول الى نظام الحجز في احد الفنادق لسرقة ارقام بطاقات الائتمان . وتتضمن بعض طوائف هذا النمط أي الكمبيوتر كهدف انشطة سرقة والاعتداء على الملكية الفكرية كسرقة الاسرار التجارية واعادة انتاج ونسخ المصنفات المحمية وتحديدا برامج الحاسوب . وفي حالات اخرى فان افعال الاختراق التي تستهدف انظمة المعلومات الخاصة تستهدف منافع تجارية او ارضاء اطماع شخصية كما ان الهدف في هذه الطائفة يتضمن انظمة سجلات طبية وانظمة الهاتف وسجلاته ونماذج تعبئة البيانات للمستهلكين وغيرها .

الثاني :- وقد يكون الكمبيوتر اداة الجريمة لارتكاب جرائم تقليدية A Tool in the commission of a traditional offense .

كما في حالة استغلال الكمبيوتر للاستيلاء على الاموال باجراء تحويلات غير مشروعة او استخدام التقنية في عمليات التزييف والتزوير ، او استخدام التقنية في الاستيلاء على ارقام بطاقات ائتمان واعادة استخدامها والاستيلاء على الاموال بواسطة ذلك ، حتى ان الكمبيوتر كوسيلة قد يستخدم في جرائم القتل ، كما في الدخول الى قواعد البيانات الصحية والعلاجية وتحويرها او تحوير عمل الاجهزة الطبية والمخبرية عبر التلاعب ببرمجياتها ، او كما في اتباع الوسائل الالكترونية للتأثير على عمل برمجيات التحكم في الطائرة او السفينة بشكل يؤدي الى تدميرها وقتل ركابها .

الثالث :- وقد يكون الكمبيوتر بيئة الجريمة ، وذلك كما في تخزين البرامج المقرصنة فيه او في حالة استخدامه لنشر المواد غير القانونية او استخدامه اداة تخزين او اتصال لصفقات ترويج المخدرات وانشطة الشبكات الاباحية ونحوها .

وطبعا يمكن للكمبيوتر ان يلعب الادوار الثلاثة معا ، ومثال ذلك ان يستخدم احد مخترقي الكمبيوتر (هاكرز) جهازه للتوصل دون تصريح الى نظام مزود خدمات انترنت (مثل نظام شركة امريكا اون لاين) ومن ثم يستخدم الدخول غير القانوني لتوزيع برنامج مخزن في نظامه (أي نظام المخترق) فهو قد ارتكب فعلا موجها نحو الكمبيوتر بوصفه هدفا (الدخول غير المصرح به) ثم استخدم الكمبيوتر لنشاط جرمي تقليدي (عرض وتوزيع المصنفات المقرصنة) واستخدم كمبيوتره كبيئة او مخزن للجريمة عندما قام بتوزيع برنامج مخزن في نظامه .

اما من حيث دور الكمبيوتر في اكتشاف الجريمة ، فان الكمبيوتر يستخدم الان على نطاق واسع في التحقيق الاستدلالي لكافة الجرائم ، عوضا عن ان جهات تنفيذ القانون تعتمد على النظم التقنية في ادارة المهام من خلال بناء قواعد البيانات ضمن جهاز ادارة العدالة والتطبيق القانوني ، ومع تزايد نطاق جرائم الكمبيوتر ، واعتماد مرتكبيها على وسائل التقنية المتجددة والمتطورة ، فانه اصبح لزاما استخدام نفس وسائل الجريمة المتطورة للكشف عنها ، من هنا يلعب الكمبيوتر ذاته دورا رئيسا في كشف جرائم الكمبيوتر وتتبع فاعليها بل وابطال اثر الهجمات التدميرية لمخترقي النظم وتحديدا هجمات الفايروسات وانكار الخدمة وقرصنة البرمجيات .

3-5 مدى كفاية التشريعات العربية لمواجهة جرائم الكمبيوتر والانترنت - تحديد عام .

تأسست قواعد حماية الاموال من مخاطر الجريمة بوجه عام على حماية المال المادي ، أي المال ذو الوجود المادي ، وكذلك التعامل مع محل الجريمة الملموس ذي الطبيعة المادية ، والتعامل ايضا مع سلوك جرمي ينتمي الى عالم السلوكيات المادية . وهذا ليس وقفا على تشريعات بعينها انما هو الاتجاه التشريعي العام لمختلف قوانين العقوبات الموضوعية ايا كان النظام القانوني الذي تنتمي اليه او يمثل مصدرا لها . وفي هذا الاطار ، فان:-

جرائم السرقة بوجه عام تقع على المال المنقول (المادي) وتتطلب فعل الاخذ او الاستيلاء (سلوك مادي) .

جرائم الاحتيال بوجه عام تتطلب سلوكا (ماديا) يهدف الى ايهام (انسان) لدفعه لتسليم مال (مادي) او ما في حكمه.

جرائم التزوير ، تتضمن تغييرا في الحقيقة عن طريق فعل مادي من حيث الاصل ، يقع على محرر (مادي) .

جرائم الاعتداء على حرمة المساكن او الاماكن الخاصة ، افعال دخول مادية (بالجسد) الى موضع ذو وجود مادي (المكان) .

جرائم اساءة الامانة او الاختلاس ، افعال استيلاء او تصرف (مادية) - من الموظف العام بالنسبة للاختلاس ، وغير الموظف بالنسبة لاساءة الائتمان - محلها المال (المادي) او ما في حكمه المحاز على سبيل الامانة (الحيازة هنا مادية) .

جرائم الاتلاف والتدمير والاعتداء على اموال الغير تنطوي على سلوكيات اضرار (مادية) توجه الى اموال (مادية).

وبالعموم فان النصوص العاقبية العربية في هذا الحقل - مع اختلاف طفيف فيما بينها بالنسبة لعناصر الجريمة واركانها - تعمل (تطبق) عند التعامل مع وقائع مادية وسلوكيات مادية تجاه محل مادي ، من هنا يتعين ان تكون محل فحص وتقييم عند الحديث عن حماية المعلومات والكيانات ذات الطبيعة المعنوية - ولا نتحدث هنا عن القيمة المالية ، لان المعلومات بحق امست ذات قيمة تفوق الموجودات المادية ، لكننا نتحدث عن طبيعة المحل وطبيعة السلوك الجرمي- هذا التقييم استهدف البحث بمدى امكان تطبيق هذه النصوص ، أي النصوص القائمة ، على الانماط الجرمية المستجدة في حقل الكمبيوتر والانترنت (جرائم الكمبيوتر والانترنت) .

ان مسألة كفاية نصوص التجريم المقررة في قوانين العقوبات التي تعالج الجرائم العادية - ولنسميها مجازا التقليدية ، لا انتقاصا من فعاليتها بل من باب مقارنتها ومقارنة نصوصها بنصوص التجريم اللازمة لمواجهة الاجرام المستجد في عالم تقنية المعلومات - كالسرقة والاختلاس والاحتيال واساءة الامانة والاتلاف والتجسس والتزوير لمواجهة انماط الاجرام المستحدثة في ميدان اجرام الحوسبة ، كانت محل جدل فقهي استمر منذ مطلع السبعينات في مختلف دول العالم ، بل امتد الجدل الى القضاء حيث حاولت بعض الاحكام انزال معطيات الكمبيوتر منزلة المال المادي المنقول وتطبيق النصوص عليه وتكييف الفعل لادخاله ضمن جرائم الاعتداء على الاموال ، وحاول جانب من الفقه والقضاء اعتبار المعطيات - بوصفها نبضات كهروبائية الكترونية - من قبيل مفهوم القوى المحرزة كالكهرباء او النبضات الهاتفية والتلغرافية ، لكن كل محاولات تطويع النصوص القائمة وليِّها لتشمل جرائم الكمبيوتر فشلت ، وكان مصير قرارات المحاكم الدنيا التي ذهبت هذا المسلك نقض احكامها من قبل المحاكم الاعلى درجة ، واذا كان المقام لا يتسع لمعالجة هذه المسألة واتجاهات الفقه تفصيلا - باعتبارها محل معالجة شمولية في الكتاب الثاني من هذه الموسوعة - فاننا نكتفي بالقول ان الدراسة التحليلية لمختلف الاتجاهات الفقهية والقضائية اظهرت قصور نصوص التجريم التقليدية السائدة عن الاحاطة بهذه الجرائم ، ومرد ذلك الى ثلاث حقائق اساسية :-

الحقيقة الاولى :- وهي التي اوضحناها اعلاه من ان جرائم الكمبيوتر تستهدف المعطيات ذات الطبيعة المعنوية ، فعندما يكون الكمبيوتر هدفا للجريمة فان السلوك يستهدف المعلومات المخزنة فيه او المنقولة منه او اليه وعندما يكون وسيلة لارتكاب الفعل ، فان السلوك يستهدف بيانات تمثل قيما مالية او اعتبارا ماليا ، ويجري الفعل او السلوك بتوسل طرق تقنية في بيئة معنوية وليست في بيئة سلوكيات مادية .
وعندما يكون بيئة للجريمة فان محتوى الفعل غير المشروع هو المعلومات غير المشروعة كما هو الحال في جرائم المحتوى المعلوماتي الضار.

الحقيقة الثانية :- ان مبدأ الشرعية الجنائية يمنع المسائلة الجنائية ما لم يتوفر النص القانوني ، فلا جريمة ولا عقوبة الا بنص ، ومتى ما انتفى النص على تجريم مثل هذه الافعال التي لا تطالها النصوص القائمة امتنعت المسؤولية وتحقق القصور في مكافحة هكذا جرائم .

الحقيقة الثالثة :- ان القياس في النصوص الجنائية الموضوعية محظور وغير جائز ، ويكاد ينحصر في الحقل الجنائي بنصوص الاجراءات الجنائية كلما كانت اصلح للمتهم ، ومؤدى ذلك امتناع قياس انماط جرائم الكمبيوتر على الجرائم التقليدية التي تستهدف الاموال والاعتبار المالي . ومن جهة اخرى لا يصلح القياس على نصوص خاصة بنوع من الجرائم كقياس سرقة المعلومات او سرقة وقت الكمبيوتر على الاستيلاء على القوى المحرزة كالكهرباء لتخلف علة القياس ولان هكذا نصوص شرعت خصيصا لتطال الانماط التي تنظمها وهي نصوص خاصة لا يتوسع في القياس عليها بل لا نبالغ ان قلنا ان جزءا من النصوص الخاصة يعد استثناءا على اصل والاستثناء لا يتوسع فيه .

هذه الحقائق التي بدت واضحة امام جهات التشريع والقضاء في النظم المقارنة بعد جدل طويل وتقييم واسع ، استدعت ان تتدخل العديد من الدول الاجنبية - التي تقارب قوانينها قوانيننا العقابية بل تعد اكثر اتساعا من قوانيننا في هذا الجانب - اقول استدعى تدخل المشرعين في هذه الدول لتعديل القوانين الجنائية او سن قوانين جديدة لمواجهة هذه الظاهرة المستجدة فبعض الدول عدلت قوانينها بالنص صراحة على انزال معطيات الكمبيوتر منزلة المال المادي المنقول وذلك لتحقق امكانية تجريم المعتدين على هذا المال بنصوص جرائم السرقة والاحتيال والاتلاف وغيرها لكن الاتجاه الغالب اتجه نحو سن تشريعات مستقلة لتجريم جرائم الكمبيوتر او استحداث نصوص مستقلة واضافتها الى تشريعاتها القائمة وهذا ، المسلك امتد ليشمل نفس الدول التي نحت المسلك الاول فعادت لسن تشريعات جديدة لعدم كفاية التعديلات التي احدثتها .

ان وضع تشريعات خاصة لمواجهة خطر جرائم الكمبيوتر يرجع الى ان تشريعات العقاب السائدة كما هو الحال في سائر التشريعات العربية تأسست على ان محل الاعتداء دائما ذو طبيعة مادية وتطلبت لحصول الجريمة وفق النموذج القانوني الاستحواذ على هذا المحل المادي ، ففي السرقة مثلا محلها الصالح للمساءلة المنقول المادي المملوك للغير الذي تم نقله والاستيلاء عليه بقصد التملك ، ومثل هذا التحديد لا يمكن ان يشمل معطيات الكمبيوتر لانها ليست منقولا ماديا ، وقد يثور الجدل حول ملكيتها ، كما ان الاستيلاء عليها او على ما تمثله لم يكن بطريق النقل والاستحواذ ، ونفس الامر يقال عن سائر الجرائم الاخرى وفق عناصرها ، فالاتلاف في القانون يقع على منقول مادي ، والتزوير يتطلب حصول التغيير في محرر ، ولا يتوفر لذاكرة الكمبيوتر صفة المحرر عند حصول تزوير او تلاعب بالبيانات المخزنة عليها ، والاحتيال يتطلب ان يقع على انسان عن طريق الايهام والتمكن من الاستيلاء على مال منقول او شيء مادي مقدر بالمال ، في حين الاحتيال في جريمة الكمبيوتر يقع على الكمبيوتر دون ايهام شخص ما او تسليم للمال وذات القول يمتد لكل جرائم القانون عند تحليل عناصرها ، لكل ذلك كان الاتجاه العام في سائر الدول المتقدم استعراض جهودها التشريعية ، النص على جرائم الاعتداء على معطيات الكمبيوتر ، يضاف الى ذلك ان القيمة الاقتصادية الاستراتيجية للمعطيات والبرامج وأهميتها في ميدان سرية نظم الدولة وبرامجها الاقتصادية والاجتماعية والسياسية والاقتصادية استلزم نصوصا رادعة تتفق وخطورة هذه الجرائم ، لهذا تصل العقوبات على بعض انواع جرائم الكمبيوتر في امريكا والمانيا واليابان الى السجن عشرين سنة .

امام هذا الواقع تعدو نصوص التجريم المقررة في قوانين العقوبات العربية عاجزة عن مواجهة خطر جرائم الكمبيوتر ، ونقصد هنا خطر الجرائم الواقعة على البيانات المالية او المتعلقة بالذمة المالية ، فاذا ما اضيف الى هذا الواقع عدم وجود نصوص تجرم افعال الاعتداء على البيانات الشخصية المخزنة في نظم المعلومات وبنوكها ، او نصوصا تحمي البيانات من خطر المعالجة الالية وتكفل حماية الخصوصية ، فاننا نكون امام واقع قاتم لن تزيل قتامته غير جهود وتدابير تشريعية حثيثة لسد النقص الحاصل وايجاد قواعد تحيط بهذا النمط الخطر والمستجد من انماط الاجرام .

اما في حقل الجرائم التي تستهدف الاعتداء على الملكية الفكرية للمصنفات الرقمية - والتي نعالجها في الفصل التالي ، فان غالبية الدول العربية نصت على الحماية الجنائية من خطر هذه الجرائم ضمن مسعى التوافق مع متطلبات الاتفاقيات العالمية وتحديدا اتفاقية (تربس - منظمة التجارة الدولية)، لكنها بالتأكيد حماية مبتسرة من جرائم الكمبيوتر سيما وانه يجري اخراج جرائم الملكية الفكرية من نطاقها باعتبارها ترد على مصنفات ابداعية تفرغ في اوعية مادية في الغالب .

6- استراتيجية حماية الخصوصية وامن المعلومات في بيئة الاعمال الالكترونية.

ما هي استراتيجية امن المعلومات Security Policy ؟

ان استراتيجية امن المعلومات ، او سياسة امن المعلومات هي مجموعة القواعد التي يطبقها الاشخاص لدى التعامل مع التقنية ومع المعلومات داخل المنشأة وتتصل بشؤون الدخول الى المعلومات والعمل على نظمها وادارتها .

ما هي اهداف استراتيجية امن المعلومات ؟

تهدف استراتيجية امن المعلومات الى :-

تعريف المستخدمين والاداريين بالتزاماتهم وواجباتهم المطلوبة لحماية نظم الكمبيوتر والشبكات وكذلك حماية المعلومات بكافة اشكالها ، وفي مراحل ادخالها ومعالجتها وخزنها ونقلها واعادة استرجاعها .

كما تهدف الاستراتيجية الى تحديد الاليات التي يتم من خلالها تحقيق وتنفيذ الواجبات المحددة على كل من له علاقة بالمعلومات ونظمها وتحديد المسؤوليات عند حصول الخطر .

بيان الاجراءات المتبعة لتجاوز التهديدات والمخاطر والتعامل معها والجهات المناط بها القيام بها بذلك .

من الذي يعد استراتيجية أمن المعلومات ؟؟

لدى اعداد اية استراتيجية بشأن امن المعلومات ، ولكي تكون هذه الاستراتيجية فاعلة ومنتجة وهادفة لا بد ان يساهم في اعدادها وتفهمها وتقبلها وتنفيذها مختلف مستويات الوظيفة في المنشأة الواحدة اضافة الى حاجتها الى التعاون والدعم الكامل من الكافة ، من هنا فان المعنيين باعداد سياسة امن المعلومات يتوزعون الى مراتب وجهات عديدة داخل المنشأة ، لكن بوجه عام تشمل مسؤولي امن الموقع ومديري الشبكات وموظفي وحدة الكمبيوتر ومديري الوحدات المختلفة في المنشأة كوحدة الاعمال والتسويق والبحث وغيرها وتشمل ايضا فريق الاستجابة للحوادث والاعطال وممثلي مجوعات المستخدمين ومستويات الادارة العليا الى جانب الادارة القانونية .

متى توصف استراتيجة امن المعلومات بانها ناجحة ؟؟

من حيث فعالية الاستخدام :- لكي توصف استراتيجية امن المعلومات بانها استراتيجة ناجحة يتعين ان تعمم بشكل شامل على كافة قطاعات الادارة وان تكون مقبولة واقعية من المناط بها تنفيذها الى جانب توفر الادلة التوجيهية والارشادية لضمان ادامة التنفيذ وعدم التقاعس فيه والتنفيذ هنا هو الاستخدام الفعلي لأدوات الحماية التقنية من جهة والتطبيق الفعلي لقواعد العمل والتعامل مع البيانات ونظمها من جهة اخرى ، ولا تحقق الاستراتيجية نجاحا ان كان ثمة غموض فيها لهذا لا بد ان تكون واضحة دقيقة في محتواها ومفهومة لدى كافة المعنيين .

أما من حيث المحتوى :- فان استراتيجة امن المعلومات تمتد الى العديد من المناحي المتصلة بنظم المعلومات وادارتها والتعامل معها اضافة الى المسائل المتعلقة بالمعلومات ذاتها وتعامل الغير مع معلومات المنشأة ، من هنا تشمل الاستراتيجية سياسة واضحة بشأن اقتناء وشراء الاجهزة التقنية وادواتها ، والبرمجيات ، والحلول المتصلة بالعمل ، والحلول المتعلقة بادارة النظام . كما تشمل استراتيجية الخصوصية المعلوماتية ، وهي التي تحدد مراتب المعلومات وقيمتها ووصفها من حيث السرية كما تبين الاستثناءات التي تعتمدها الاستراتيجية على حق الخصوصية لموظفي المنشأة مع مبررات هذه الاستثناءات ، كرقابة البريد الالكتروني مثلا او رقابة الدخول الى المنشأة او رقابة الوصول الى ملفات المستخدمين بالمنشأة . ومن حيث الدخول الى الشبكات والمعلومات فلا بد من استراتيجية دخول واضحة تحدد حقوق وامتيازات كل شخص في المنشأة للوصول الى ملفات او مواقع معينة في النظام اضافة الى سياسة بشأن التعامل مع الاتصالات الخارجية ، المعطيات اجهزة ووسائل الاتصال المستخدمة ، اضافة البرامج الجديدة ، استراتيجيات المراسلة مع الاخرين .

وتضم استراتيجية المعلومات ايضا استراتيجية الاشتراكات التي تحدد سياسة المنشأة بشأن اشتراكات الغير في شبكتها او نظمها ، وكذلك استراتيجيات التعامل مع المخاطر والاخطاء بحيث تحدد ماهية المخاطر واجراءات ابلاغ عنها والتعامل معها والجهات المسؤولة عن التعامل مع هذه المخاطر .

ما هي منطلقات واساس استراتجية امن المعلومات ؟؟

يتعين ان تنطلق استراتيجة امن المعلومات من تحديد المخاطر ، اغراض الحماية ، ومواطن الحماية ، وانماط الحماية اللازمة ، واجراءات الوقاية من المخاطر ، وتتلخص المنطلقات والاسس التي تبنى عليها استراتيجية امن المعلومات القائمة على الاحتياجات المتباينة لكل منشأة من الاجابة عن تساؤلات ثلاث رئيسة :-

ماذا اريد ان احمي ؟؟

مِن ماذا احمي المعلومات ؟؟

كيف احمي المعلومات ؟؟

اغراض حماية البيانات الرئيسة .

1 - السرية CONFIDENTIALITY : التأكد من ان المعلومات لا تكشف ولا يطلع عليها من قبل اشخاص غير مخولين بذلك .

2 - التكاملية وسلامة المحتوى INTEGRITY : التأكد من ان محتوى المعلومات صحيح لم يتم تعديله او العبث به وبشكل خاص لن يتم تدمير المحتوى او تغيره او استطعانه او عن طريق تدخل غير مشروع .

3 - استمرارية توفر المعلومات او الخدمة AVAILABILITY :- التأكد من ان مستخدم المعلومات لن يتعرض الى انكار استخدامه لها او دخوله اليها .

مناطق امن المعلومات

1 - امن الاتصالات : ويراد بأمن الاتصالات حماية المعلومات خلال عملية تبادل البيانات من نظام الى اخر

2 - امن الكمبيوتر : ويراد به حماية المعلومات داخل النظام بكافة انواعها وانماطها كحماية نظام التشغيل و حماية برامج التطبيقات وحماية برامج ادارة البيانات وحماية قواعد البيانات بانواعها المختلفة .

ولا يتحقق امن المعلومات دون توفير الحماية المتكاملة لهذين القطاعين عبر معايير امنية تكفل توفير هذه الحماية ، ومن خلال مستويات امن متعددة ومختلفة من حيث الطبيعة .

انماط ومستويات امن المعلومات

1 - الحماية المادية : وتشمل كافة الوسائل التي تمنع الوصول الى نظم المعلومات وقواعدها كالاقفال والحواجز والغرف المحصنة وغيرها من وسائل الحماية المادية التي تمنع الوصول الى الاجهزة الحساسة .

2- الحماية الشخصية : وهي تتعلق بالموظفين العاملين على النظام التقني المعني من حيث توفير وسائل التعريف الخاصة بكل منهم وتحقيق التدريب والتأهيل للمتعاملين بوسائل الامن الى جانب الوعي بمسائل الامن ومخاطر الاعتداء على المعلومات .

3 - الحماية الادارية : ويراد بها سيطرة جهة الادارة على ادارة النظم المعلومات وقواعدها مثل التحكم بالبرمجيات الخارجية او الاجنبية عن المنشأة ، ومسائل التحقيق باخلالات الامن ، ومسائل الاشراف والمتابعة لأنشطة الرقابة اضافة الى القيام بانشطة الرقابة ضمن المستويات العليا ومن ضمنها مسائل التحكم بالاشتراكات الخارجية .

4 - الحماية الاعلامية- المعرفية : كالسيطرة على اعادة انتاج المعلومات وعلى عملية اتلاف مصادر المعلومات الحساسة عند اتخاذ القرار بعدم استخدامها .

المخاطر

هناك مخاطر عديدة يمكن ان تواجه نظام المعلومات بما في ذلك انظمة التجارة الالكترونية وابرز هذه المخاطر ما يلي :

1 - اختراق الانظمة : ويتحقق ذلك بدخول شخص غير مخول بذلك الى نظام الكمبيوتر والقيام بأنشطة غير مصرح له بها كتعديل البرمجيات التطبيقية وسرقة البيانات السرية او تدمير الملفات او البرمجيات او النظام او لمجرد الاستخدام غير المشروع . ويتحقق الاقتحام بشكل تقليدي

من خلال انشطة (التقنيع والتخفي) ويراد به تظاهر الشخص المخترق بانه شخص اخر مصرح له بالدخول . او من خلال استغلال نقاط الضعف في النظام كتجاوز اجراءات السيطرة والحماية او من خلال المعلومات التي يجمعها الشخص المخترق من مصادر مادية او معنوية ، كالتنقيب في قمامة المنشأة للحصول على كلمات السر او معلومات عن النظام او عن طريق الهندسة الاجتماعية كدخول الشخص الى مواقع معلومات حساسة داخل النظام ككلمات السر او المكالمات الهاتفية .

2 - الاعتداء على حق التخويل : ويتم من خلال قيام الشخص المخول له استخدام النظام لغرض ما باستخدامه في غير هذا الغرض دون ان يحصل على التخويل بذلك ، وهذا الخطر يعد من الأخطار الداخلية في حقل اساءة استخدام النظام من قبل موظفي المنشأة ، وهو قد يكون ايضا من الاخطار الخارجية ، كاستخدام المخترق حساب شخص مخول له باستخدام النظام عن طريق تخمين كلمة السر الخاصة به او استغلال نقطة ضعف بالنظام للدخول اليه بطريق مشروع او من جزء مشروع ومن ثم القيام بانشطة غير مشروعة .

3 - زراعة نقاط الضعف : عادة ينتج هذا الخطر عن اقتحام من قبل شخص غير مصرح له بذلك او من خلال مستخدم مشروع تجاوز حدود التخويل الممنوح له بحيث يقوم الشخص بزرع مدخل ما يحقق له الاختراق فيما بعد . ومن اشهر امثلة زراعة المخاطر حصان طرواد ، وهو عبارة عن برنامج يؤدي غرضا مشروعا في الظاهر لكنه يمكن ان يستخدم في الخفاء للقيام بنشاط غير مشروع ، كان يستخدم برنامج معالجة كلمات ظاهريا لتحرير وتنسيق النصوص في حين يكون غرضه الحقيقي طباعة كافة ملفات النظام ونقلها الى ملف مخفي بحيث يمكن للمخترق ان يقوم بطباعة هذا الملف والحصول على محتويات النظام .

4 - مراقبة الاتصالات : بدون اختراق كمبيوتر المجني عليه يتمكن الجاني من الحصول على معلومات سرية غالبا ما تكون من المعلومات التي تسهل له مستقبلا اختراق النظام وذلك ببساطة من خلال مراقبة الاتصالات من احدى نقاط الاتصال او حلقاتها .

5 - اعتراض الاتصالات : وكذلك بدون اختراق النظام يقوم الجاني في هذه الحالة باعتراض المعطيات المنقولة خلال عملية النقل ويجري عليها التعديلات التي تتناسب مع غرض الاعتداء ، ويشمل اعتراض الاتصالات قيام الجاني بخلق نظام وسيط وهمي بحيث يكون على المستخدم ان يمر من خلاله ويزود النظام بمعلومات حساسة بشكل طوعي .

6 - انكار الخدمة : ويتم ذلك من خلال القيام بأنشطة تمنع المستخدم الشرعي من الوصول الى المعلومات او الحصول على الخدمة وابرز انماط انكار الخدمة ارسال كمية كبيرة من رسائل البريد الالكتروني دفعة واحدة الى موقع معين بهدف اسقاط النظام المستقبل لعدم قدرته على احتمالها او توجيه عدد كبير من عناوين الانترنت على نحو لا يتيح عملية تجزئة حزم المواد المرسلة فتؤدي الى اكتظاظ الخادم وعدم قدرته على التعامل معه .

7 - عدم الاقرار بالقيام بالتصرف : ويتمثل هذا الخطر في عدم اقرار الشخص المرسل اليه او المرسل بالتصرف الذي صدر عنه ، كأن ينكر انه ليس هو شخصيا الذي قام بارسال طلب الشراء عبر الانترنت

الوقاية من مخاطر الاعتداء على المعلومات

في ميدان حماية الاتصالات وحماية الكمبيوتر يعبر عن اجراءات الوقاية بخدمات الامن ، ولا يقصد بها الخدمات بالمعنى المعروف ، وانما اطلق هذا التعبير جراء نشوء شركات متخصصة بأمن المعلومات تقدم هذه الخدمات ، وبالعموم فان هناك خمسة انواع اساسية لخدمات الأمن تستهدف حماية خمسة عناصر رئيسة في ميدان المعلومات وهي :

1 - خدمات (وسائل) حماية التعريف Identification and Authentication هذه الخدمات تهدف الى التثبت من الهوية وتحديدا عندما يقوم شخص ما بالتعريف عن نفسه فان هذه الخدمات تهدف الى التثبت من انه هو الشخص نفسه ولهذا فان التعريف يعد الوسائل التي تحمي من انشطة التخفي والتنكر ومن هنا فان هناك نوعين من خدمات التعريف الاول تعريف الشخصية واشهر وسائلها كلمات السر وثانيها التعريف بأصل المعلومات كالتثبت من أصل الرسالة .

2 - خدمات (وسائل) السيطرة على الدخول Access Control : وهذه الخدمات تستخدم للحماية ضد الدخول غير المشروع الى مصادر الانظمة والاتصالات والمعلومات ويشمل مفهوم الدخول غير المصرح به لأغراض خدمات الامن الاستخدام غير المصرح به والافشاء غير المصرح به ، والتعديل غير المصرح به ، والاتلاف غير المصرح به ، واصدار المعلومات والاوامر غير المصرح بها ولهذا فان خدمات التحكم بالدخول تعد الوسائل الاولية لتحقيق التخويل والتثبت منه .

3 - خدمات (وسائل) السرية Data and message Confidentiality: هذه الخدمات تحمي المعلومات من الافشاء للجهات غير المصرح لها بالحصول عليها ، والسرية تعني بشكل عام اخفاء المعلومات من خلال تشفيرها على سبيل المثال او من خلال وسائل اخرى كمنع التعرف على حجمها او مقدارها او الجهة المرسلة اليها .

4 - خدمات (وسائل) حماية التكاملية وسلامة المحتوى Data and message Integrity: هذه الخدمات تهدف الى حماية مخاطر تغيير البيانات خلال عمليات ادخالها او معالجتها او نقلها وعملية التغيير تعني بمفهوم الامن هنا الالغاء او التحوير او اعادة تسجيل جزء منها او غير ذلك وتهدف هذه الوسائل ايضا الى الحماية من انشطة تدمير المعطيات بشكل كامل او الغاءها دون تخويل .

5 - خدمات (وسائل) منع الانكار Non-repudiation: وهذه الخدمات تهدف الى منع الجهة التي قامت بالتصرف من انكار حصول نقل البيانات او النشاط من قبلها .

وتعد الخدمات الخمس المتقدمة مناطق الحماية الاساسية في حقل المعلومات ، فالحماية يتعين ان تمتد الى التعريف ، انشطة الدخول ، السرية ، سلامة المحتوى ، منع عدم الانكار .

ماذا عن استراتجية امن الانترنت ؟؟؟

تنصب استراتيجة أمن المعلومات في حقل تحقيق أمن الانترنت على مواضع ثلاث :- أمن الشبكة ، أمن التطبيقات ، أمن النظم . وكل منها ينطوي على قواعد ومتطلبات تختلف عن الاخرى ويتعين ان تكون انظمة الامن في هذه المواضع الثلاث متكاملة مع بعضها حتى تحقق الوقاية المطلوبة لانها بالعموم تنطوي ايضا على اتصال وارتباط بمستويات الامن العامة كالحماية المادية والحماية الشخصية والحماية الادارية والحماية الاعلانية . وفيما تقدم اشرنا الى العناصر المتصلة بأمن النظم والبرمجيات والمعطيات وبقي ان نشير في هذا المقام الى امن الشبكات -:

ان ما يحمى من خلال امن الشبكة هو عملية الاتصال والتبادل بين احد كمبيوترات الشبكة (النظام النهائي سواء اكان نظام الزبون ان نظام المستضيف (الخادم) وبين كمبيوتر اخر ضمن الشبكة ، فاذا ارتبط النظام النهائي بالانترنت مباشرة دون وجود وسائل امن ما بين هذا النظام والشبكة فان اية حزمة بيانات مرسلة قد يلحق بها ما يلي :

أ - قد يتم تغيرها خلال عملية النقل

ب - قد لا تظهر من حيث مصدرها من الجهة التي قدمت منها

ج - قد تكون جزء من هجوم يستهدف النظام

د - قد لا تصل الى العنوان المرسلة اليه

هـ - قد يتم قراءتها والاطلاع عليها وافشاءها من الغير .

ويهدف أمن الشبكات من جهة اخرى الى حماية الشبكة نفسها واظهار الثقة لدى مستخدم النظام النهائي بتوفر وسائل الحماية في تعامله مع الشبكة وكذلك اظهار الشبكة ذاتها بانها تحتوى على وسائل امن لا تتطلب معها ان يكون كمبيوتر المستخدم محتويا على وسائل خاصة .

وتتضمن وسائل امن الشبكة ما يلي : -

1 - التعريف والسلامة من خلال تزويد نظام المستقبل بالثقة في حماية حزم المعلومات والتأكد من ان المعلومات التي وصلت لم يتم تعديلها .

2 - السرية : حماية محتوى حزم المعلومات من الافشاء الا للجهات المرسلة اليها .

3 - التحكم بالدخول : تقيد الاتصالات بحصرها ما بين النظام المرسل والنظام المستقبل .

ما هي مرتكزات الاستراتيجية التشريعية الوطنية لحماية المعلومات؟

إن السياسة التشريعية في مجال الأفعال المعتبرة جرائم كمبيوتر وجرائم انترنت ، يفترض أن تؤسس على أن المصلحة التي يحميها القانون هي الحق في المعلومات وفق توازن يراعى كفالة تدفقها وتنظيم معالجتها واستخدامها ونقلها، وعلى أن موضوع جريمة الكمبيوتر ومحل الاعتداء المباشر هو المعطيات بدلالتها التقنية الشاملة.

في التعامل مع المعلوماتية يتعين ادراك ما يحصل من تحول في السلوكيات من مادية الى معنوية ، وما نشهده من تحول من اقتصاد الموجودات الى اقتصاد المعلومات ، مما يتطلب ان تكون مرتكزات الحماية وقواعد التنظيم مؤسسة على الاهمية المتنامية للقيم المعنوية وحاجة الاخيرة الى الاعتراف بها وسن قواعد تتواءم مع طبيعتها .

اذا كان الجدل والنقاش أساسه مدى امكان انطباق نصوص القوانين الجنائية التقليدية على الجرائم التي تستهدف الاعتداء على معطيات الكمبيوتر أو المعلومات، الذي خلق مواقف فقهية ترفض ذلك أو تؤيده أو ترى عدم كفايته من جهة وامكان تحققه من نواح أخرى، والذي امتد الى القضاء وحتى جهات التشريع ، لم يكن بمقدوره اضعاف القناعة السائدة لدى العموم :- أولا ، بالطبيعة الخاصة لموضوع جرائم الكمبيوتر - المعطيات. وثانيا ، بالطبيعة المعنوية للمعلومات والمعطيات التي لم تكن فيما سبق محلا للحماية الجنائية أو مثارا لتشييد نظريات تتفق وطبيعتها.12

ان هاتين الحقيقتان، الطبيعة المادية للحقوق المالية التي يحميها القانون الجنائي، والطبيعة المعنوية لمعطيات الحاسوب ، خلقتا اتجاهات متباينة في تحديد الطبيعة القانونية للمعلومات (معطيات الحاسوب)، فظهر اتجاه فقهي - الفقه الفرنسي تحديدا- "يعتبر المعلومات أموالا ذات طبيعة خاصة انطلاقا من ان غياب الكيان المادي للمعلومات لا يجعلها محلا لحق مالي من نوع الحقوق المتعارف عليها في الفقه والتي ترد على كيانات مادية، وان جاز اعتبارها محلا لحق ملكية ادبية أو فنية أو صناعية، وبالتالي فان المعلومات التي لا تكون متصلة بالنواحي الأدبية والفنية والصناعية أو التي تأبى بطبيعتها أن تكون محلا لمثل هذه الحقوق، يلزم بالضرورة استبعادهما من طائفة الأموال، وليس من مقتضى هذا الاستبعاد - ان تظل المعلومات خارج نطاق أية حماية اذا ما جرى الاستيلاء عليها أو استخدامها استخداما غير مشروع ، فمثل هذا الفعل يعد (خطأ) يحرك مسؤولية فاعله، والسائد لدى جانب من الفقه الفرنسي ان هذه المسؤولية تتحرك وفق قواعد المسئولية المدنية المستندة الى نص المادة 1382/ من القانون المدني الفرنسي، وبالاعتراف بالخطأ تكون المحكمة قد اعترفت بوجود الحق وهو "الحق في المعلومات" مما مؤداه أن يكون للمعلومات طبيعة خاصـــة تسمـــح بأن يكـــون الحق الوارد عليها من نوع الملكية العلمية.

أما فيما يتعلق بالمعلومات ونظمها وسبل معالجتها آليا، فان الأمر في رأينا لا ينبغي أن يترك للتفسير الفقهي والقضائي من أجل بسط النصوص القائمة على الاستيلاء على المعلومات على نحو ما فعل الفقه والقضاء في فرنسا في بادئ الامر ، وقد شقي في ذلك..ان الأيسر والأصوب ان يلتفت المشرع الى هذه المشكلة بتشريع خاص ينص على تجريم صور العدوان المتصورة على المعلومات ونظمها وبرامجها وسبل معالجتها، فهذه الصور غير مقصورة على الاستيلاء على المعلومات بقصد الغش فقط، بل انها تشمل الكثير مما ينبغي التصدي له بتجريم وبعقاب يتناسب مع الأضرار المتوقعة من صور العدوان المختلفة هذه، والتي يواصل التقدم العلمي الكشف عنها يوما بعد يوم . ولنا في تراجع الدول المتقدمة عن تطويع النصوص القائمة وقيامها بسن تشريعات بديلة عبرة تساعد في حسم الموقف من آليات الحماية التشريعية المطلوبة .13

يؤدي ظهور الحق في المعلومات بالنسبة للقانون الجنائي الموضوعي (قانون العقوبات) الى محورين أساسيين للمشكلة : أولا، انه من الضروري البحث عن مدى حماية المالك أو حائز المعلومات في الأنظمة القانونية الوطنية المختلفة، ثانيا :- يجب الاحاطة بتفاصيل حماية الحياة الخاصة للفرد المعني بفحوى المعلومات .

ما هو محتوى الاستراتيجية التشريعية الوطنية لحماية المعلومات؟

الاعتراف بالحق في المعلومات ، انسيابها وتدفقها وتداولها .

تحديد مفهوم معلومات الكمبيوتر / المعطيات / البرامج / البيانات لجهة تحديد نطاق الحماية ومحله .

اعتماد معايير قياسية ورقابية بشأن الخدمات التقنية / الإنترنت / مقاهي الإنترنت / البريد الإلكتروني / التجارة الإلكترونية / البنوك الالكترونية ... الخ

تحديد معايير الموثوقية والسرية والاستمرارية اللازمة لمعالجة وتداول البيانات وتحديدا في طور نقلها .

---

12 يقول الفقيه (Huet) " انه من الصعوبة بمكان، ان توفر الجرائم التقليدية (والأدق نصوص التجريم التقليدية) - المرتكـــزة على التفكير في تحقيق ثروة فعلية أو اتلاف مستندات مادية - حماية فعالة لهـــذه القيـــم المعنـــوية التي تمخض عنها المعلوماتية" ويقول الفقيه (H. CROZE) " يمكن القول بداءة بأن المعلومات - باعتبارها عنصرا من عناصر المعرفة - ليس لها طبيعة مادية".

13 يقول الفقيه الالماني Ulrich Sieber: "تعكس نقطة الانطلاق المستحدثة (للحق في المعلومات) حقيقة مضمونها، ان التقدير القانوني للأموال المادية يجب أن يختلف عن نظيره بالنسبة للأموال المعنوية، ويتعلق أول مظهر للخلاف بحماية المالك أو الحائز للأموال المادية أو المعنوية، وفي حين أن الأموال المادية نظرا لطبيعتها يستأثر بها شخص محدد على نحو مطلق، فان المعلومات بالأحرى هي مال شائع، ومن ثم يجب أن تكون من حيث المبدأ حرة ولا يجب أن تحمى بالحقوق الاستئثارية والتي تقتصر على الأموال المادية، ويعد هذا المبدأ الأساس (حرية الوصول للمعلومات) شرطا جوهريا لأي نظام اقتصادي وسياسي حر، وعلاوة على ذلك، فهو في غاية الأهمية من أجل تقدم الدول التي في طريقها للتنمية. وترجع الخاصية الثانية لتقدير الأموال المادية والمعنوية، الى أن حماية المعلومات يجب أن لا ينظر اليها بوصفها تمثل مصالح الأشخاص الذين تأثروا بفحوى المعلومات، ويبرر هذا الوجه، القيود المستحدثة في نطاق حماية الحياة الخاصة في مجال تقنية المعلومات، وقد صار من الواضح اذن، أنه يستحيل تقليل القوانين التشريعية الخاصة بتقنية المعلومات قياسا على النصوص الخاصة بالأموال المادية، ولكن يجب زيادة الأسس الخاصة بها". واذا كانت أفكار الفقيه Ulrich المتقدمة، مما يتصل بأسس السياسة التشريعية في نطاق الحماية الجنائية للمعلومات المفترض تأسيسها على حماية الحق في المعلومات، بمراعاة حرية انسيابها وتدفقها واستخدامها من جهة، والحماية الجنائية لمواجهة أنشطة الاعتداء على المعلومات. فانها في الوقت ذاته تعطي انطباعا واضحا عن وجوب مغايرة الرؤى لآليات حماية المعطيات عن آليات حماية الأموال المادية المنطلقة أساسا من الاعتراف بطبيعتها الخاصة، ومراعاة ماهيتها وخصائصها وخصائص الجرائم الواقعة عليها.

تحديد انماط السلوك الاجرامي في ميدان التقنية العالية وبشكل رئيس جرائم الاتصالات وشبكات المعلومات . مع اعتماد الحد الادنى المقرر في التشريعات المقارنة من صور جرائم التقنية العالية واعتماد تدابير ردعية واحترازية تتناسب معها ، كل ذلك بما يتلائم مع الواقع الوطني ومرتكزات النظام القانوني الاردني والموائمة مع السائد من نظريات القانون العامة ومستويات تفريد العقاب للجرائم المنصوص عليها في القسم الخاص خاصة جرائم الاموال والجرائم الاقتصادية .

اتخاذ التدابير التشريعية في ميدان البينات والاثبات والادلة والقواعد الاجرائية المتناسبة مع طبيعة هذه الجرائم بما لا يخل بالحقوق الدستورية وقواعد المشروعية الاجرائية والحق في الخصوصية .

ما هي متطلبات نجاح وفعالية الاستراتيجية التشريعية الوطنية لحماية المعلومات ؟

اعتماد استراتيجيات تدريبية امنية لإعداد القضاة والمحامين والضابطة العدلية بشان جرائم التقنية العالية تحقيقها وكشفها واثباتها .

اعتماد استراتيجية وطنية لحماية الابداع الوطني في حقل البرمجيات والمخترعات التقنية وعدم الانشغال بحماية الاجنبي على حساب تشجيع الابداع الوطني الذي يكفل لنا انتاج المعارف لا استهلاكها .

اعداد البنية الادارية المناسبة لقيادة مؤسسات التقنية في عصر المعلومات.

اشاعة الوعي بين الافراد والمؤسسات لأهمية التعاون بخصوص كشف الاختراقات الامنية ومواجهتها وعدم اخفائها ، واشاعة الثقة بقدرة الأجهزة الامنية على كشف هذه الانماط الجرمية المستحدثة .

اعتماد الدراسة البحثية المقارنة بخصوص حاجة التشريعات الوطنية الموضوعية والاجرائية للإحاطة بالانماط المستجدة من الجرائم في ميدان التقنية العالية .

هل تتغير الاستراتيجيات ام تتغير محتوى مراحلها التطبيقية ؟؟

مع تطور العمل على نحو متسارع بسبب تطورات عصر المعلومات المذهلة ، قد يكون التغيير الذي يطرا على المنشأة جوهريا وقد يكون متسارعا لكن لا احد يتنبه الى مدى التغيير واثره ، وكقاعدة عامة فان التغيير الجوهري يستلزم اعادة تقييم للاستراتيجيات الاساسية وليس فقط الجوانب المتغيرة والتطبيقية من الاستراتيجية . وعلينا ان ندرك حقيقة ان القدرة على اقامة نظام فاعل لامن المعلومات – تقنيا وتنظيميا وقانونيا- يستلزم القدرة العالية على مواكبة المتغيرات التي لا تعني هنا تغيير الاجهزة والوسائل فقط مجاراة للحديث وعروض البيع ووسائل التسويق والموضة ، انها تعني عقلية متغيرة تدرك الجديد وتثق بتوافر المكنات لمواجهته وتحديه .

7- الخلاصة والتوصيات

في بيئة الاعمال الالكترونية عموما ، واعمال الهواتف الخلوية الالكترونية علينا ان ندرك حقيقة ان الحماية القانونية تعدل باهميتها بل تفوق وفرة البنى التحتية وخطط الاستثمار ، وتحقيق الحماية القانونية ليس متيسرا دون وجود نظام قانوني فاعل لمواجهة مخاطر امن المعلومات في هذه البيئة ومواجهة مخاطر الاعتداء على خصوصية سرية بيانات الافراد والمؤسسات .

اننا في هذه المناسبة ندعو الى الوقوف امام التشرعيات القائمة في النظام القانوني واعادة قراءة قدؤتها على التواؤم مع متطلبات هذه الاعمال تمهيدا لاصدار حزمة معتبرة ومتكاملة من القواعد التي تفي بتنظيم اعمال الهواتف الخليوة او الوسائل اللاسلكية الالكترونية .

وفي الوقت نفسه ، فان المصارف العربية مدعوة لتبني استراتيجيات عمل واضحة ، تغطي الابعاد الاستثمارية والتقنية والقانونية لاستخدامات للهواتف الخليوية والوسائل اللاسلكية في العمل المصرفي .

وان اهم واعظم الحلول فعالية تلك التي تراعي الواقع القائم وتدرك جيدا احتياجاته دون الوقع في منزلق الحلول والتدابير الجاهزة .